

SafeGuard Enterprise
Administratorhilfe



Produktversion: 7
Stand: Dezember 2014

Inhalt

1 Über SafeGuard Enterprise 7.0

SafeGuard Enterprise bietet umfassenden Schutz von Daten durch Verschlüsselung und zusätzlicher Authentisierung für die Anmeldung.

Diese Version von SafeGuard Enterprise unterstützt Windows 7 und Windows 8 auf Endpoints mit BIOS oder UEFI.

- Für Systeme mit BIOS können Sie zwischen SafeGuard Enterprise Festplattenverschlüsselung und von SafeGuard Enterprise verwalteter BitLocker Verschlüsselung wählen. Die BIOS Version verwendet den BitLocker-eigenen Wiederherstellungsmechanismus.

  Hinweis: Wenn in diesem Handbuch von SafeGuard Power-on Authentication oder SafeGuard Festplattenverschlüsselung die Rede ist, dann bezieht sich das nur auf Windows 7 BIOS Endpoints.

- Für UEFI Systeme verwenden Sie die von SafeGuard Enterprise verwaltete BitLocker Verschlüsselung für die Festplattenverschlüsselung. Für diese Endpoints bietet SafeGuard Enterprise verbesserte Challenge/Response Funktionalitäten. Nähere Informationen zu den unterstützten UEFI-Versionen und Beschränkungen hinsichtlich der Unterstützung von SafeGuard BitLocker Challenge/Response finden Sie in den Versionshinweisen unter http://downloads.sophos.com/readmes/readsgn_7_eng.html.

Hinweis: Wenn sich die Beschreibung nur auf UEFI bezieht, ist das explizit angegeben.

Die Tabelle zeigt, welche Komponenten verfügbar sind.

	SafeGuard Festplattenverschlüsselung mit SafeGuard Power-on Authentication (POA)	BitLocker mit Pre-Boot Authentication (PBA), von SafeGuard verwaltet	SafeGuard C/R Wiederherstellung für BitLocker Pre-Boot Authentication (PBA)
Windows 7 BIOS	**JA**	**JA**	
Windows 7 UEFI		**JA**	**JA**
Windows 8 BIOS		**JA**	
Windows 8 UEFI		**JA**	**JA**
Windows 8.1 BIOS		**JA**	
Windows 8.1 UEFI		**JA**	**JA**

Hinweis: SafeGuard C/R Wiederherstellung für BitLocker Pre-Boot Authentication (PBA) ist nur auf 64 bit Systemen verfügbar.

SafeGuard Festplattenverschlüsselung mit SafeGuard Power-on Authentication (POA) ist das Sophos Modul zur Verschlüsselung von Laufwerken auf Endpoints. Es wird mit einer von Sophos entwickelten Pre-Boot Authentication namens SafeGuard Power On Authentication

(POA) geliefert, die Anmeldeoptionen wie Smartcard und Fingerabdruck sowie einen Challenge/Response Mechanismus für die Wiederherstellung unterstützt.

BitLocker mit Pre-Boot Authentication (PBA), von SafeGuard verwaltet, ist die Komponente, die das BitLocker Verschlüsselungsmodul und die BitLocker Pre-Boot Authentication aktiviert und verwaltet.

Sie ist für BIOS und UEFI Plattformen verfügbar:

- Die UEFI Version bietet zusätzlich einen SafeGuard Challenge/Response Mechanismus für die BitLocker Wiederherstellung für den Fall, dass Benutzer ihre Kennwörter vergessen. Die UEFI Version kann verwendet werden, wenn bestimmte Plattform-Anforderungen erfüllt sind. Beispielsweise muss die UEFI Version 2.3.1 sein. Nähere Informationen entnehmen Sie bitte den Versions-Infos.
- Die BIOS Version bietet die Wiederherstellungs-Erweiterungen des SafeGuard Challenge/Response Mechanismus nicht. Sie dient auch als Fallback falls die Anforderungen an die UEFI Version nicht erfüllt sind. Der Sophos Installer prüft, ob die Voraussetzungen erfüllt sind. Falls nicht, installiert er automatisch die BitLocker Version ohne Challenge/Response.

Mac Endpoints

Für Mac Endpoints sind folgende Produkte verfügbar: Sie werden auch von SafeGuard Enterprise verwaltet oder berichten zumindest an das Management Center.

	Sophos SafeGuard File Encryption for Mac 7.0	Sophos SafeGuard Native Device Encryption (FileVault 2-Verwaltung) 7.0
OS X 10.8	**JA**	**JA**
OS X 10.9	**JA**	**JA**
OS X 10.10	**JA**	**JA**

Die Beschreibungen in diesem Handbuch beziehen sich ausschließlich auf Windows. Für die Mac Versionen sehen Sie bitte in den entsprechenden Produkt-Handbüchern nach.

Sophos Mobile Encryption

Mit **Sophos Mobile Encryption** können Sie Dateien lesen, die von den SafeGuard Enterprise-Modulen **SafeGuard Cloud Storage** oder **SafeGuard Data Exchange** verschlüsselt wurden. Sie können Dateien mit einem lokalen Schlüssel verschlüsseln. Diese lokalen Schlüssel sind von einer Passphrase abgeleitet, die von einem Benutzer eingegeben wurde. Sie können eine Datei nur entschlüsseln, wenn Sie die Passphrase kennen, die zur Verschlüsselung der Datei verwendet wurde. Nähere Informationen zu Sophos Mobile Encryption finden Sie unter www.sophos.com/de-de.

2 Empfohlene Sicherheitsmaßnahmen

Wenn Sie die hier beschriebenen, einfachen Schritte befolgen, reduzieren Sie Risiken und die Daten auf Ihrem Computer sind jederzeit sicher und geschützt.

Für Informationen zur zertifizierungsgerechten Anwendung von SafeGuard Enterprise finden Sie im *SafeGuard Enterprise Manual for certification-compliant operation* (Englisch).

Vermeiden Sie den Standbymodus.

Wenn sich SafeGuard Enterprise-geschützte Endpoints in bestimmten Energiesparmodi befinden, in denen das Betriebssystem nicht ordnungsgemäß heruntergefahren und bestimmte Hintergrundprozesse nicht beendet werden, besteht die Gefahr, dass sich Angreifer Zugriff auf die Verschlüsselungsschlüssel verschaffen. Der Schutz kann erhöht werden, wenn das Betriebssystem immer vollständig heruntergefahren oder in den Ruhezustand versetzt wird.

Informieren Sie die Benutzer entsprechend oder erwägen Sie, den Standbymodus auf nicht benutzten Endpoints zentral zu deaktivieren:

- Vermeiden Sie den Standbymodus ebenso wie den hybriden Standbymodus. Der hybride Standbymodus ist eine Mischung aus Energiesparmodus und Standbymodus. Die Einstellung einer zusätzlichen Kennwort-Abfrage nach dem Aufwecken des Computers bietet keinen vollen Schutz.

- Vermeiden Sie das Sperren von Desktops, das Ausschalten von Monitoren oder das Zuklappen von Laptops, wenn darauf kein vollständiges Herunterfahren oder der Ruhezustand folgt. Die Einstellung einer zusätzlichen Kennwort-Abfrage nach dem Aufwecken des Computers bietet keinen ausreichenden Schutz.

- Fahren Sie stattdessen die Endpoints herunter oder versetzen Sie sie in den Ruhezustand. Beim nächsten Benutzen des Computers wird stets die SafeGuard Power-on Authentication aktiviert, die somit vollen Schutz bietet.

  Hinweis: Es ist wichtig, dass sich die Ruhezustand-Datei auf einem verschlüsselten Volume befindet. Normalerweise liegt sie auf Laufwerk C:\.

  Die entsprechenden Einstellungen für die Energieverwaltung können Sie zentral mit Gruppenrichtlinienobjekten oder lokal im **Eigenschaften für Energieoptionen** Dialog in der **Systemsteuerung** des Endpoints konfigurieren. Stellen Sie die Aktion für die **Standbymodus** Schaltfläche auf **Ruhezustand** oder **Herunterfahren**.

Setzen Sie eine Richtlinie für sichere Kennwörter um.

Setzen Sie eine Richtlinie für sichere Kennwörter um und erzwingen Sie einen Kennwortwechsel in regelmäßigen Abständen, besonders für die Anmeldung an Endpoints.

Kennwörter sollten nicht an andere Personen weitergegeben oder aufgeschrieben werden.

Informieren Sie Benutzer, wie sie sichere Kennwörter wählen. Ein sicheres Kennwort folgt diesen Regeln:

- Es ist lange genug um sicher zu sein: Eine Mindestlänge von 10 Zeichen ist zu empfehlen.
- Es enthält eine Mischung aus Buchstaben (Groß- und Kleinschreibung), Zahlen und Sonderzeichen/Symbolen.

- Es enthält keine allgemein gebräuchlichen Wörter oder Namen.
- Es ist schwer zu erraten, aber es ist leicht, es sich zu merken und korrekt einzutippen.

Deaktivieren Sie die SafeGuard Power-on Authentication nicht.

Die SafeGuard Power-on Authentication bietet zusätzlichen Schutz für die Anmeldung am Endpoint. Sie wird mit der Festplattenverschlüsselung von SafeGuard Enterprise installiert und standardmäßig aktiviert. Um vollen Schutz zu gewährleisten, deaktivieren Sie die Power-on Authentication nicht. Weitere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/110282.aspx

Schutz vor dem Einschleusen von Code

Unter Umständen ist das Einschleusen von Code (zum Beispiel DLL Pre-Loading-Angriffe) möglich, wenn es einem Angreifer gelingt, schädlichen Code (zum Beispiel in ausführbaren Dateien) in Verzeichnisse einzubringen, in denen die SafeGuard Enterprise Verschlüsselungssoftware nach legitimem Code sucht. So wenden Sie diese Bedrohung ab:

- Installieren Sie die von der Verschlüsselungssoftware geladene Middleware, zum Beispiel Token Middleware, in Verzeichnissen, auf die externe Angreifer nicht zugreifen können. Dies sind üblicherweise die Unterverzeichnisse der **Windows** und **Programme** Verzeichnisse.
- Die PATH-Umgebungsvariable sollte keine Komponenten enthalten, die auf Ordner verweisen, auf die externe Angreifer zugreifen können (siehe oben).
- Reguläre Benutzer sollten keine Administratorenrechte haben.

Best Practices für die Verschlüsselung

- **Stellen Sie sicher, dass allen Laufwerken ein Laufwerksbuchstabe zugewiesen ist.**

  Nur Laufwerke, die einen Laufwerksbuchstaben zugewiesen haben, können verschlüsselt/entschlüsselt werden. Folglich können Laufwerke ohne Laufwerksbuchstaben missbraucht werden, um an vertrauliche Daten im Klartext zu gelangen.

  So wenden Sie diese Bedrohung ab: Erlauben Sie den Benutzern nicht, die Laufwerkbuchstabenzuweisungen zu ändern. Konfigurieren Sie die Benutzerrechte entsprechend. Reguläre Benutzer haben dieses Recht standardmäßig nicht.

- **Gehen Sie bei der Anwendung der schnellen Initialverschlüsselung vorsichtig vor.**

  SafeGuard Enterprise bietet die schnelle Initialverschlüsselung zur Beschleunigung der Initialverschlüsselung von Volumes. Dies wird dadurch erreicht, dass nur auf den Speicherplatz zugegriffen wird, der tatsächlich in Gebrauch ist. Dieser Modus kann zu einem unsichereren Zustand führen, wenn ein Volume vor der Verschlüsselung mit SafeGuard Enterprise bereits in Gebrauch war. Aufgrund Ihres Aufbaus sind Solid State Disks (SSD) hier stärker betroffen als reguläre Festplatten. Dieser Modus ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/113334.aspx.

- **Verwenden Sie nur den Algorithmus AES-256 für die Datenverschlüsselung.**
- **Verwenden Sie SSL/TLS (SSL Version 3 oder höher) für den Schutz der Kommunikation zwischen Client und Server.**

  Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

- **Verhindern Sie die Deinstallation.**

  Um Endpoints zusätzlich zu schützen, kann die lokale Deinstallation von SafeGuard Enterprise über eine Richtlinie mit **spezifischen Computereinstellungen** verhindert werden. Setzen Sie das Feld **Deinstallation erlaubt** auf **Nein** und übermitteln Sie die Richtlinie an die Endpoints. Versuche, die Software zu deinstallieren, werden abgebrochen und die nicht autorisierten Versuche werden protokolliert.

  Wenn Sie eine Demoversion benutzen, setzen Sie vor Ablauf der Demoversion die Option **Deinstallation erlaubt** auf **Ja**.

  Wenden Sie den Sophos Manipulationsschutz auf Endpoints an, auf denen Sophos Endpoint Security and Control installiert ist.

3 Über das SafeGuard Management Center.

Das SafeGuard Management Center ist das zentrale Instrument für die Verwaltung von mit SafeGuard Enterprise verschlüsselten Computern. Mit dem SafeGuard Management Center können Sie eine unternehmensweite Sicherheitsstrategie implementieren und auf Endpoints anwenden. Im SafeGuard Management Center können Sie:

- Organisationsstruktur aufbauen oder importieren.
- Sicherheitsbeauftragte anlegen.
- Richtlinien definieren.
- Konfigurationen exportieren und importieren.
- Computer mit einer umfassenden Protokollierungsfunktionalität überwachen.
- Kennwörter und den Zugriff auf verschlüsselte Endpoints wiederherstellen.

Mit dem SafeGuard Management Center wird Multi Tenancy für die Verwaltung von mehreren Domänen und Datenbanken unterstützt. Sie können verschiedene SafeGuard Enterprise Datenbanken verwalten und unterschiedliche Konfigurationen verwenden.

Der Zugriff auf das SafeGuard Management Center ist nur privilegierten Benutzern - den Sicherheitsbeauftragten - erlaubt. Es können mehrere Sicherheitsbeauftragte gleichzeitig mit den Daten arbeiten. Die verschiedenen Sicherheitsbeauftragten können entsprechend den ihnen zugewiesenen Rollen und Rechten Tätigkeiten ausführen.

Sie können die SafeGuard Enterprise Richtlinien und Einstellungen an Ihre Anforderungen anpassen. Nach dem Speichern der neuen Einstellungen in der Datenbank können diese an die Endpoints übertragen werden, wo sie dann wirksam werden.

Hinweis: Einige Features sind nicht in allen Lizenzen enthalten. Für Informationen dazu, was in Ihrer Lizenz enthalten ist, wenden Sie sich an Ihren Vertriebspartner.

4 Anmeldung am SafeGuard Management Center

Während der Erstkonfiguration von SafeGuard Enterprise wird ein Konto für einen Haupt-Sicherheitsbeauftragten angelegt. Dieses Konto wird bei der ersten Anmeldung an das SafeGuard Management Center benötigt. Um das SafeGuard Management Center zu starten, benötigt der Benutzer das Kennwort für den Zertifikatsspeicher sowie den privaten Schlüssel des Zertifikats.

Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

Die Anmeldung richtet sich danach, ob Sie das SafeGuard Management Center mit einer Verbindung zu einer Datenbank (Single Tenancy) oder zu mehreren Datenbanken (Multi Tenancy) einsetzen.

Hinweis: Zwei Sicherheitsbeauftragte dürfen nicht das gleiche Windows-Konto auf einem Computer benutzen. Andernfalls lassen sich ihre Zugriffsrechte nicht sauber trennen.

4.1 Warnung bei Ablauf des Unternehmenszertifikats

Sechs Monate vor Ablauf des Unternehmenszertifikats zeigt das SafeGuard Management Center bei der Anmeldung eine Warnung an und fordert Sie dazu auf, das Zertifikat zu erneuern und an die Endpoints zu übertragen. Ohne gültiges Unternehmenszertifikat können Endpoints keine Verbindung mit dem Server herstellen.

Sie können das Unternehmenszertifikat jederzeit erneuern. Dies ist auch dann möglich, wenn das Unternehmenszertifikat bereits abgelaufen ist. Wenn ein Unternehmenszertifikat abgelaufen ist, wird dies auch durch eine Meldung angegeben. Informationen zum Erneuern des Unternehmenszertifikats finden Sie unter Erneuerung des Unternehmenszertifikats (Seite 84).

4.2 Anmeldung im Single Tenancy Modus

1. Starten Sie das SafeGuard Management Center über den Produktordner im **Start** Menü. Ein Anmeldebildschirm wird angezeigt.
2. Melden Sie sich als Haupt-Sicherheitsbeauftragter an und geben Sie das Zertifikatsspeicherkennwort ein, das während der Konfiguration festgelegt wurde. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

4.3 Anmeldung im Multi Tenancy Modus

Wenn Sie mehrere Datenbanken konfiguriert haben (Multi Tenancy), erweitert sich der Vorgang der Anmeldung am SafeGuard Management Center (siehe Mit mehreren Datenbankkonfigurationen arbeiten (Seite 33)).

1. Starten Sie das SafeGuard Management Center über den Produktordner im **Start** Menü. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Wählen Sie die Datenbankkonfiguration, die Sie verwenden möchten, aus der Dropdownliste und klicken Sie auf **OK**.

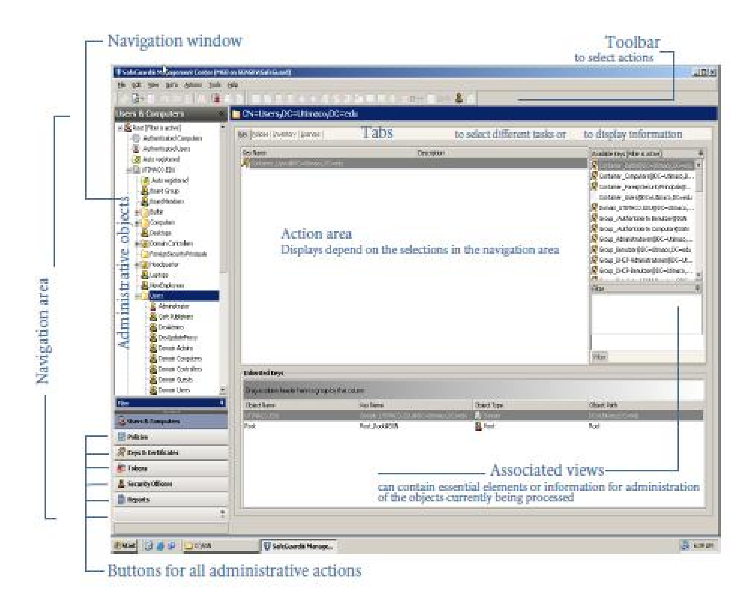
   Die ausgewählte Datenbankkonfiguration wird mit dem SafeGuard Management Center verbunden und wird aktiv.

3. Zur Anmeldung an das SafeGuard Management Center werden Sie dazu aufgefordert, den Namen des Sicherheitsbeauftragten für diese Konfiguration auszuwählen und Ihr Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

Hinweis: Wenn Sie ein falsches Kennwort eingeben, wird eine Fehlermeldung angezeigt und die nächste Anmeldung wird verzögert. Diese Verzögerung wird mit jedem fehlgeschlagenen Anmeldeversuch größer. Fehlgeschlagene Anmeldeversuche werden protokolliert.

4.4 SafeGuard Management Center Benutzeroberfläche



Navigationsbereich:

Im Navigationsbereich befinden sich Schaltflächen für alle administrativen Tätigkeiten:

- **Benutzer und Computer**

Zum Importieren von Gruppen und Benutzern aus einem Active Directory, aus der Domäne oder von einem einzelnen Computer.

- **Richtlinien**

  Zum Erzeugen der Richtlinien.

- **Schlüssel und Zertifikate**

  Zum Verwalten der Schlüssel und Zertifikate.

- **Token**

  Zur Verwaltung von Token und Smartcards.

- **Sicherheitsbeauftragte**

  Zum Anlegen neuer Sicherheitsbeauftragter und Definieren von Aktionen, für deren Ausführung eine zusätzliche Autorisierung notwendig ist.

- **Berichte**

  Zum Anlegen und Verwalten von Berichten zu sicherheitsrelevanten Ereignissen.

Navigationsfenster

Im Navigationsfenster werden Objekte zur Bearbeitung angezeigt (Active Directory Objekte wie OUs, Benutzer und Computer; Richtlinien usw.) bzw. können dort erstellt werden. Welche Objekte angezeigt werden, hängt vom ausgewählten Vorgang ab.

Hinweis: Unter **Benutzer & Computer** werden die Objekte in der Baumstruktur des Navigationsfensters in Abhängigkeit von den Zugriffsrechten des Sicherheitsbeauftragten für Verzeichnisobjekte angezeigt. Die Baumstruktur zeigt nur die Objekte, auf die der angemeldete Sicherheitsbeauftragte Zugriff hat. Objekte, für die der Zugriff verweigert wird, werden nicht angezeigt, es sei denn, es sind weiter unten in der Baumstruktur Knoten vorhanden, für die der Sicherheitsbeauftragte Zugriffsrechte hat. In diesem Fall werden die Objekte, für die der Zugriff verweigert wird, ausgegraut. Wenn der Sicherheitsbeauftragte das Zugriffsrecht **Voller Zugriff** hat, wird das jeweilige Objekt schwarz dargestellt. Objekte mit Zugriffsrecht **Schreibgeschützt**, werden blau dargestellt.

Aktionsbereich

Im Aktionsbereich nehmen Sie die Einstellungen für das im Navigationsfenster ausgewählte Objekt vor. Im Aktionsbereich stehen verschiedene Registerkarten zur Verfügung mit deren Hilfe die Objekte bearbeitet und die Einstellungen vorgenommen werden können.

Informationen zu den ausgewählten Objekten werden ebenfalls im Aktionsbereich angezeigt.

Dazugehörige Ansichten (Associated Views)

In diesen Ansichten werden zusätzliche Objekte und Informationen angezeigt. Diese geben einerseits nützliche Informationen bei der Verwaltung des Systems und unterstützen die einfache Bedienung. Sie können zum Beispiel Objekten Schlüssel per Drag and Drop zuweisen.

Symbolleiste

Hier befinden sich Symbole für die verschiedenen Aktionen im SafeGuard Management Center. Die Symbole werden eingeblendet, wenn sie für das ausgewählte Objekt zur Verfügung stehen.

Nach der Anmeldung wird das SafeGuard Management Center immer in der Ansicht gestartet, in der es geschlossen wurde.

4.5 Sprache der Benutzeroberfläche

Sie können die Sprache der Benutzeroberfläche während der Installation des SafeGuard Management Center sowie der SafeGuard Enterprise Verschlüsselungssoftware am Endpoint steuern.

Sprache des SafeGuard Management Center

So stellen Sie die Sprache das SafeGuard Management Center ein:

- Klicken Sie in der SafeGuard Management Center Menüleiste auf **Extras > Optionen > Allgemein**. Klicken Sie auf **Benutzerdefinierte Sprache verwenden** und wählen Sie eine verfügbare Sprache aus. Die Sprachen Englisch, Deutsch, Französisch und Japanisch werden unterstützt.

- Starten Sie das SafeGuard Management Center neu. Er wird in der ausgewählten Sprache angezeigt.

SafeGuard Enterprise Oberflächensprache auf Endpoints

Die Sprache von SafeGuard Enterprise auf dem Endpoint steuern Sie über den Richtlinientyp **Allgemeine Einstellungen** im SafeGuard Management Center (Einstellung, **Anpassung > Sprache am Client**):

- Wenn die Sprache des Betriebssystems gewählt wird, richtet sich die Produktsprache nach der Spracheinstellung des Betriebssystems. Steht die entsprechende Betriebssystemsprache in SafeGuard Enterprise nicht zur Verfügung, wird standardmäßig die englische Version von SafeGuard Enterprise angezeigt.

- Wenn eine der zur Verfügung stehenden Sprachen gewählt wird, werden die SafeGuard Enterprise Funktionen auf dem Endpoint in der ausgewählten Sprache angezeigt.

5 Konfigurieren des SafeGuard Management Center

Nach der Installation müssen Sie das SafeGuard Management Center konfigurieren. Der SafeGuard Management Center Konfigurationsassistent unterstützt Sie bei der Erstkonfiguration durch Hilfestellung bei der Definition der grundlegenden SafeGuard Management Center Einstellungen sowie bei der Konfiguration der Datenbankverbindung. Der Assistent wird automatisch aufgerufen, wenn Sie das SafeGuard Management Center zum ersten Mal nach der Installation starten.

Sie können das SafeGuard Management Center für die Anwendung mit einer oder mehreren Datenbank (Multi Tenancy) konfigurieren.

Hinweis: Die folgenden Schritte müssen mit dem Konfigurationsassistenten sowohl für Single Tenancy als auch für Multi Tenancy Konfigurationen ausgeführt werden.

5.1 Voraussetzungen

Folgende Voraussetzungen müssen erfüllt sein:

- Stellen Sie sicher, dass Sie über Windows Administratorrechte verfügen.
- Halten Sie die folgenden Informationen bereit. Diese erhalten Sie ggf. von Ihrem SQL-Administrator.
  - SQL Anmeldeinformationen.
  - Name des SQL Servers, auf dem die SafeGuard Enterprise Datenbank laufen soll.
  - Name der SafeGuard Enterprise Datenbank, falls diese bereits erzeugt wurde.

5.2 Multi Tenancy Konfigurationen

Sie können mehrere verschiedene SafeGuard Enterprise Datenbankkonfigurationen für eine Instanz des SafeGuard Management Center konfigurieren und verwalten. Dies erweist sich vor allem dann als nützlich, wenn Sie verschiedene Konfigurationen für verschiedene Domänen, Organisationseinheiten oder Unternehmensstandorte einsetzen möchten.

Hinweis: Sie müssen pro Datenbank (Mandant) jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

Zur Vereinfachung der Konfiguration können neu erstellte Datenbankkonfigurationen zur späteren Wiederverwendung in eine Datei exportiert werden und zuvor erstellte Konfigurationen aus einer Datei eingelesen werden.

Um das SafeGuard Management Center für Multi Tenancy zu konfigurieren, führen Sie zunächst die initiale Konfiguration und danach weitere spezifische Schritte für die Multi Tenancy Konfiguration durch.

5.3 Starten der Erstkonfiguration des SafeGuard Management Centers

Nach der Installation des SafeGuard Management Center, müssen Sie die Erstkonfiguration durchführen. Die Erstkonfiguration muss sowohl für den Single Tenancy als auch für den Multi Tenancy Modus ausgeführt werden.

So starten Sie den SafeGuard Management Center Konfigurationsassistenten:

1. Starten Sie das **SafeGuard Management Center** über das **Start** Menü. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
2. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.

5.4 Konfigurieren der Datenbankserver-Verbindung

Zum Speichern aller SafeGuard Enterprise spezifischen Verschlüsselungsrichtlinien und Einstellungen wird eine Datenbank verwendet. Damit das SafeGuard Management Center mit dem SafeGuard Enterprise Server kommunizieren kann, müssen Sie eine Authentisierungsmethode für den Zugriff auf die Datenbank festlegen, entweder Windows NT Authentisierung oder SQL-Authentisierung. Wenn Sie eine Verbindung zum Datenbankserver mit SQL Authentisierung herstellen möchten, stellen Sie sicher, dass Sie die notwendigen SQL-Anmeldedaten zur Hand haben. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

1. Führen Sie auf der Seite **Datenbankserver-Verbindung** folgende Schritte aus:
   - Wählen Sie unter **Verbindungseinstellungen** den SQL-Datenbankserver aus der **Datenbankserver** Liste aus. Es werden alle Rechner eines Netzwerks aufgelistet, auf denen ein Microsoft SQL Server installiert ist. Wenn der Server nicht auswählbar ist, tragen Sie Servername bzw. IP-Adresse mit dem SQL-Instanznamen manuell ein.
   - Aktivieren Sie **SSL verwenden**, um die Verbindung zwischen SafeGuard Management Center und SQL-Datenbankserver zu sichern. Wenn Sie **SQL Server Authentisierung** ausgewählt haben, empfehlen wir dringend, diese Einstellung zu aktivieren, da dadurch der Transport der SQL-Anmeldedaten verschlüsselt wird. SSL-Verschlüsselung erfordert eine funktionsfähige SSL-Umgebung auf dem SQL-Datenbankserver, die Sie vorab einrichten müssen (siehe Sichern von Transportverbindungen mit SSL (Seite 41)).
2. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf die Datenbankserverinstanz benutzt werden soll. Dies ist erforderlich, damit das SafeGuard Management Center mit der Datenbank kommunizieren kann:
   - Aktivieren Sie **Windows NT Authentisierung verwenden**, um Ihre Windows-Anmeldedaten zu verwenden.

     Hinweis:

     Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer Teil einer Domäne ist. In diesem Fall sind jedoch zusätzliche Konfigurationsschritte notwendig, da der Benutzer dazu berechtigt sein muss, eine Verbindung mit der Datenbank herzustellen. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung.*

- Aktivieren Sie **SQL Server Authentisierung verwenden**, um mit den entsprechenden SQL-Anmeldeinformationen auf die Datenbank zuzugreifen. Geben Sie die Anmeldeinformationen des SQL-Benutzerkontos ein, das Ihr SQL-Administrator erstellt hat. Falls notwendig, erhalten Sie diese Informationen von Ihrem SQL Administrator.

  Hinweis:

  Verwenden Sie diese Art der Authentisierung, wenn Ihr Computer keiner Domäne angehört. Aktivieren Sie **SSL verwenden**, um die Verbindung zum und vom Datenbankserver zu sichern.

3. Klicken Sie auf **Weiter**.

Die Verbindung zum Datenbankserver ist hergestellt.

5.5 Erstellen oder Auswählen einer Datenbank

Hinweis: Wenn Sie SafeGuard Enterprise und SafeGuard LAN Crypt parallel verwenden, verwenden Sie verschiedene Datenbanken.

Legen Sie auf der Seite **Datenbankeinstellungen** fest, ob eine existierende Datenbank oder eine neue Datenbank zum Speichern der Administrationsdaten benutzt werden soll.

1. Gehen Sie wie folgt vor:

   - Wenn noch keine Datenbank existiert, wählen Sie **Eine neue Datenbank mit folgendem Namen erstellen**. Geben Sie einen Namen für die neue Datenbank ein. Sie benötigen dazu die entsprechenden SQL-Zugriffsberechtigungen. Weitere Informationen hierzu finden Sie in der SafeGuard Enterprise Installationsanleitung. Um Probleme zu vermeiden, sollten in SafeGuard Enterprise Datenbanknamen nur folgende Zeichen verwendet werden: Buchstaben (A - Z, a - z), Zahlen (0 - 9), Unterstriche (_).

   - Wenn bereits eine Datenbank angelegt wurde oder wenn Sie das SafeGuard Management Center bereits auf einem anderen Computer installiert haben, klicken Sie auf **Folgende bestehende Datenbank wählen** und wählen Sie die entsprechende Datenbank aus der Liste aus.

2. Klicken Sie auf **Weiter**.

5.6 Erstellen eines Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO)

Als Sicherheitsbeauftragter melden Sie sich am SafeGuard Management Center an, um SafeGuard Enterprise Richtlinien zu erstellen und die Verschlüsselungssoftware für die Endbenutzer zu konfigurieren.

Der Haupt-Sicherheitsbeauftragte (MSO) ist der Administrator höchster Ebene mit allen Rechten und einem Zertifikat, das nicht abläuft.

1. Geben Sie auf der Seite **Daten des Sicherheitsbeauftragten** unter **Haupt-Sicherheitsbeauftragten-ID** einen Namen für den Haupt-Sicherheitsbeauftragten ein.

2. Führen Sie auf der Seite **Zertifikat für den Haupt-Sicherheitsbeauftragten** einen der folgenden Schritte aus:

   - Klicken Sie auf **Erzeugen**, um ein neues Zertifikat für den Haupt-Sicherheitsbeauftragten zu erzeugen. Sie werden dazu aufgefordert, sowohl für den Zertifikatsspeicher als auch für die Datei, in die das Zertifikat exportiert werden soll (private Schlüsseldatei P12), jeweils ein Kennwort einzugeben und zu bestätigen. Das Zertifikat wird erzeugt und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

   - Klicken Sie auf **Importieren**, um ein Zertifikat für den Haupt-Sicherheitsbeauftragten zu verwenden, das bereits auf dem Netz zur Verfügung steht. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Schlüsseldatei. Geben Sie unter**Kennwort für die Schlüsseldatei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Geben Sie das Kennwort für den Zertifikatsspeicher unter **Kennwort des Zertifikatsspeichers** ein und bestätigen Sie es. Klicken Sie auf **OK**. Das Zertifikat wird erzeugt und unter **Zertifikat für den Haupt-Sicherheitsbeauftragten** angezeigt.

   Der Haupt-Sicherheitsbeauftragte benötigt das Kennwort des Zertifikatsspeichers für die Anmeldung am SafeGuard Management Center. Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Steht das Kennwort nicht mehr zur Verfügung, so kann sich der Haupt-Sicherheitsbeauftragte nicht mehr am SafeGuard Management Center anmelden.

   Für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt der Haupt-Sicherheitsbeauftragte die private Schlüsseldatei.

3. Klicken Sie auf **Weiter**.

Der Haupt-Sicherheitsbeauftragte wird angelegt.

5.6.1 Erzeugen des Zertifikats des Haupt-Sicherheitsbeauftragten

Gehen Sie in **Zertifikat des Haupt-Sicherheitsbeauftragten erzeugen** folgendermaßen vor:

1. Bestätigen Sie unter **Haupt-Sicherheitsbeauftragten-ID** den Namen des Haupt-Sicherheitsbeauftragten.
2. Geben Sie nun zweimal das Kennwort für den Zertifikatsspeicher ein und klicken Sie auf **OK**.

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird erzeugt und lokal als Backup (<mso_name>.cer) gespeichert.

Hinweis: Notieren Sie sich das Kennwort und bewahren Sie es an einem sicheren Ort auf. Sie benötigen es für die Anmeldung am SafeGuard Management Center.

5.6.2 Export des Zertifikats des Haupt-Sicherheitsbeauftragten

Das Zertifikat des Haupt-Sicherheitsbeauftragten wird in eine Datei exportiert, die so genannte private Schlüsseldatei (P12). Diese ist mit einem Kennwort gesichert. Das Zertifikat des Haupt-Sicherheitsbeauftragten ist dadurch zusätzlich geschützt. Die private Schlüsseldatei wird für die Wiederherstellung einer beschädigten SafeGuard Management Center Installation benötigt.

So exportieren Sie das Zertifikat eines Haupt-Sicherheitsbeauftragten:

1. Geben Sie unter **Zertifikat exportieren** ein Kennwort für den privaten Schlüssel (P12-Datei) ein und bestätigen Sie es. Das Kennwort muss aus 8 alphanumerischen Zeichen bestehen.
2. Klicken Sie auf **OK**.

3. Geben Sie einen Speicherort für die private Schlüsseldatei ein.

Die private Schlüsseldatei wird erzeugt und die Datei wird am angegebenen Speicherort gespeichert <mso_name.p12).

Hinweis: Erstellen Sie eine Sicherungskopie des privaten Schlüssels (P12-Datei) und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab. Andernfalls führt ein eventueller PC-Absturz zum Verlust des Schlüssels und SafeGuard Enterprise muss neu installiert werden. Das gilt für alle von SafeGuard Enterprise generierten Sicherheitsbeauftragten-Zertifikate. Weitere Informationen finden Sie in der Administrator-Hilfe im Kapitel *Unternehmenszertifikat und Master Security Officer Zertifikat exportieren*.

5.6.3 Import des Zertifikats des Haupt-Sicherheitsbeauftragten

Wenn bereits ein Zertifikat eines Haupt-Sicherheitsbeauftragten zur Verfügung steht, müssen Sie es in den Zertifikatsspeicher importieren.

Hinweis: Ein Zertifikat kann nicht aus einer Microsoft PKI importiert werden. Ein importiertes Zertifikat muss minimal 1024 Bits haben und kann maximal 4096 Bits lang sein.

1. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die **[...]** Schaltfläche und wählen Sie die Schlüsseldatei aus.
2. Geben Sie das Kennwort der Schlüsseldatei ein.
3. Geben Sie das Kennwort für den Zertifikatsspeicher ein.
4. Bestätigen Sie das Kennwort für den Zertifikatsspeicher.
5. Klicken Sie auf **OK**.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

5.7 Erzeugen des Unternehmenszertifikats

Mit dem Unternehmenszertifikat lassen sich unterschiedliche SafeGuard Management Center Installationen auseinander halten. In Verbindung mit dem Zertifikat des Haupt-Sicherheitsbeauftragten lässt sich mit dem Unternehmenszertifikat eine beschädigte SafeGuard Enterprise Datenbankkonfiguration wiederherstellen.

1. Wählen Sie auf der Seite **Unternehmenszertifikat** die Option **Neues Unternehmenszertifikat erzeugen**.

   Hinweis: Erzeugte Unternehmenszertifikate laufen immer am 31. Dezember 2199 ab.

2. Geben Sie einen Namen Ihrer Wahl ein.

   Hinweis: Von SafeGuard Enterprise erzeugte Zertifikate, zum Beispiel Unternehmens-, Maschinen-, Sicherheitsbeauftragten- und Benutzerzertifikate, sind bei einer Erstinstallation standardmäßig zur Erweiterung der Sicherheit mit dem Hash-Algorithmus **SHA-256** signiert.

   Wenn Sie noch SafeGuard Enterprise Endpoints mit Version 6 oder einer früheren Version mit dem SafeGuard Management Center der Version 7.0 verwalten müssen, müssen Sie unter **Hash-Algorithmus für erzeugte Zertifikate** den Algorithmus **SHA-1** auswählen. Weitere Informationen finden Sie im Abschnitt *Ändern des Algorithmus für selbst-signierte Zertifikate*.

   Der ausgewählte Algorithmus wird zum Signieren aller von SafeGuard Enterprise erzeugten Zertifikate benutzt. Dies sind die Unternehmens- und Maschinenzertifikate sowie die Sicherheitsbeauftragten- und Benutzerzertifikate.

3. Klicken Sie auf **Weiter**.

Das neu angelegte Unternehmenszertifikat wird in der Datenbank gespeichert.

Erstellen Sie eine Sicherungskopie des Unternehmenszertifikats und legen Sie diese direkt nach der Erstkonfiguration an einem sicheren Speicherort ab.

Informationen zur Wiederherstellung einer beschädigten Datenbankkonfiguration finden Sie unter Wiederherstellung einer beschädigten Datenbankkonfiguration (Seite 262).

5.8 Abschließen der Erstkonfiguration des SafeGuard Management Centers

1. Klicken Sie auf **Beenden**, um die Erstkonfiguration des SafeGuard Management Center abzuschließen.

Eine Konfigurationsdatei wurde erzeugt:

- Eine Verbindung zum SafeGuard Enterprise Server.
- Eine SafeGuard Enterprise Datenbank.
- Ein Haupt-Sicherheitsbeauftragten-Konto für die Anmeldung an das SafeGuard Management Center.
- Alle notwendigen Zertifikate für die Wiederherstellung einer beschädigten Datenbankkonfiguration oder SafeGuard Management Center Installation

Sobald der Konfigurationsassistent geschlossen ist, wird das SafeGuard Management Center gestartet.

5.9 Erstellen weiterer Datenbankkonfigurationen (Multi Tenancy)

Voraussetzung: Die Funktion Multi Tenancy muss über eine Installation vom Typ **Vollständig** installiert worden sein. Die initiale Konfiguration des SafeGuard Management Center muss durchgeführt worden sein.

Hinweis: Sie müssen pro Datenbank jeweils eine separate SafeGuard Enterprise Server Instanz einrichten.

So erstellen Sie eine weitere SafeGuard Enterprise Datenbankkonfiguration nach der Erstkonfiguration:

1. Starten Sie das SafeGuard Management Center. Der Dialog **Konfiguration auswählen** wird angezeigt.
2. Klicken Sie auf **Neu**. Der SafeGuard Management Center Konfigurationsassistent wird automatisch gestartet.
3. Der Assistent führt Sie durch die notwendigen Schritte für das Anlegen einer neuen Datenbankkonfiguration. Nehmen Sie die erforderlichen Einstellungen vor. Die neue Datenbankkonfiguration wird generiert.
4. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden. Wenn Sie das SafeGuard Management Center das nächste Mal starten, können Sie die neue Datenbank-Konfiguration aus der Liste auswählen.

5.10 Konfigurieren zusätzlicher Instanzen des SafeGuard Management Center

Sie können zusätzliche Instanzen des SafeGuard Management Center konfigurieren, um Sicherheitsbeauftragten den Zugriff für die Durchführung administrativer Aufgaben auf verschiedenen Computern zu ermöglichen. Das SafeGuard Management Center kann auf jedem Rechner im Netzwerk installiert sein, von wo aus auf die Datenbank zugegriffen werden kann.

SafeGuard Enterprise verwaltet die Zugriffsrechte auf das SafeGuard Management Center in einem eigenen Zertifikatsverzeichnis. In diesem Verzeichnis müssen die Zertifikate aller Sicherheitsbeauftragten, die sich am SafeGuard Management Center anmelden dürfen, vorhanden sein. Für die Anmeldung an das SafeGuard Management Center ist dann nur das Kennwort für den Zertifikatsspeicher erforderlich.

1. Installieren Sie SGNManagementCenter.msi mit den gewünschten Features auf einem weiteren Computer.
2. Starten Sie das SafeGuard Management Center auf dem Computer mit dem neu installierten SafeGuard Management Center. Der Konfigurationsassistent wird gestartet und führt Sie durch die notwendigen Schritte.
3. Klicken Sie auf der **Willkommen** Seite auf **Weiter**.
4. Wählen Sie im Dialog **Datenbankverbindung** unter **Datenbankserver** die erforderliche SQL-Datenbankinstanz aus der Liste aus. Alle auf Ihrem Computer oder Netzwerk verfügbaren Datenbankserver werden angezeigt. Wählen Sie unter **Authentisierung** die Art der Authentisierung, die für den Zugriff auf diese Datenbankinstanz benutzt werden soll. Wenn Sie **SQL Server Authentisierung verwenden** wählen, geben Sie die SQL-Benutzerkontenanmeldedaten ein, die Ihr SQL-Administrator erstellt hat. Klicken Sie auf **Weiter**.
5. Aktivieren Sie unter **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus. Klicken Sie auf **Weiter**.
6. Wählen Sie unter **SafeGuard Management Center Authentisierung** eine autorisierte Person aus der Liste aus. Wenn Multi Tenancy aktiviert ist, zeigt der Dialog an, an welcher Konfiguration sich der Benutzer anmeldet. Geben Sie das Kennwort für den Zertifikatsspeicher ein und bestätigen Sie es.

   Der Zertifikatsspeicher für das aktuelle Benutzerkonto wird angelegt und ist durch dieses abgesichert. Für die nachfolgenden Anmeldungen benötigen Sie nur noch dieses Kennwort.

7. Klicken Sie auf **OK**.

   Eine Meldung, dass Zertifikat und privater Schlüssel nicht gefunden bzw. nicht darauf zugegriffen werden kann, wird angezeigt.

8. Klicken Sie zum Importieren der Daten auf **Ja** und dann auf **OK**. Dadurch wird der Importvorgang gestartet.

9. Klicken Sie unter **Authentisierungs-Schlüsseldatei importieren** auf die **[...]** Schaltfläche und wählen Sie die Schlüsseldatei aus. Geben Sie das **Kennwort der Schlüsseldatei** ein. Geben Sie das zuvor unter **Kennwort des Zertifikatsspeichers oder Token-PIN** definierte Kennwort für den Zertifikatsspeicher ein. Wählen Sie **In den Zertifikatsspeicher importieren** oder **Auf den Token kopieren**, um das Zertifikat auf einem Token zu speichern.
10. Geben Sie zur Initialisierung des Zertifikatsspeichers das Kennwort noch einmal ein.

Zertifikat und privater Schlüssel befinden sich nun im Zertifikatsspeicher. Zur Anmeldung an das SafeGuard Management Center wird das Kennwort des Zertifikatsspeichers verwendet.

6 Lizenzen

Für die Nutzung von SafeGuard Enterprise mit dem SafeGuard Management Center im produktiven Betrieb ist eine gültige Lizenz erforderlich. So ist eine gültige Lizenz in der SafeGuard Enterprise Datenbank zum Beispiel die Voraussetzung für die Übertragung von Richtlinien an die Endpoints. Darüber hinaus sind für die Token-Verwaltung die entsprechenden Token-Lizenzen notwendig.

Sie erhalten Lizenzdateien von Ihrem Vertriebspartner. Diese Dateien müssen nach der Installation in die SafeGuard Enterprise Datenbank importiert werden.

Die Lizenzdatei enthält u. a. folgende Informationen:

- Anzahl an erworbenen Lizenzen pro Modul
- Kundenname
- Einen festgelegten Toleranzwert für die Überschreitung der Anzahl an erworbenen Lizenzen

Bei Überschreiten der verfügbaren Lizenzen bzw. des Toleranzlimits werden beim Starten des SafeGuard Management Centers entsprechende Warnungs- bzw. Fehlermeldungen ausgegeben.

Für die Lizenzverwaltung bietet das SafeGuard Management Center im Bereich **Benutzer & Computer** einen Überblick zum Lizenzstatus des installierten SafeGuard Enterprise Systems. Der Lizenzstatusüberblick steht in der Registerkarte **Lizenzen** für den Stamm-Knoten, für Domänen, OUs, Containerobjekte und Arbeitsgruppen zur Verfügung. Sicherheitsbeauftragte erhalten hier detaillierte Informationen zum Lizenzstatus. Mit der entsprechenden Berechtigung können sie Lizenzen in die SafeGuard Enterprise Datenbank importieren.

6.1 Lizenzdatei

Die Lizenzdatei, die Sie zum Import in die SafeGuard Enterprise Datenbank erhalten, ist eine .XML-Datei mit Signatur. Sie enthält folgende Informationen:

- Kundenname
- Zusätzliche Informationen (zum Beispiel Abteilung, Niederlassung)
- Datum, an dem die Lizenz ausgestellt wurde.
- Anzahl an Lizenzen pro Modul
- Token-Lizenzinformationen
- Lizenzablaufdatum
- Lizenztyp (Demo- oder Voll-Lizenz)
- Signatur mit Lizenzsignaturzertifikat

6.2 Token-Lizenzen

Für die Verwaltung von Token bzw. Smartcards sind die entsprechenden zusätzlichen Token-Lizenzen erforderlich. Wenn diese Lizenzen nicht zur Verfügung stehen, können Sie im SafeGuard Management Center keine Richtlinien für Token erstellen.

6.3 Evaluierungs- und Demo-Lizenzen

Es besteht die Möglichkeit, für Evaluierungs- oder initiale Rollout-Prozesse die Standard-Lizenzdatei (Evaluierungslizenz) oder individuelle Demo-Lizenzdateien zu nutzen. Diese Lizenzen sind nur für einen bestimmten Zeitraum gültig und haben ein Ablaufdatum, die Funktionalität ist jedoch in keinster Weise eingeschränkt.

Hinweis: Evaluierungs- und Demo-Lizenzen dürfen nicht für den regulären produktiven Betrieb von SafeGuard Enterprise Modulen genutzt werden.

6.3.1 Standard-Lizenzdateien

Bei der Installation des SafeGuard Management Centers wird automatisch eine Standard-Lizenzdatei geladen. Diese Evaluierungslizenz mit der Bezeichnung SafeGuard Enterprise Evaluation License enthält jeweils fünf Lizenzen pro Modul und hat eine zeitlich begrenzte Gültigkeitsdauer von zwei Jahren ab dem Release-Datum der jeweiligen SafeGuard Enterprise Version.

Standard-Lizenzdatei für SafeGuard Cloud Storage und SafeGuard File Encryption

Bei der Installation von SafeGuard Management Center 7 wird automatisch eine zusätzliche Standard-Lizenzdatei für SafeGuard Cloud Storage und SafeGuard File Encryption geladen. Diese Evaluierungslizenz enthält fünf Lizenzen für jedes der beiden Module und hat eine zeitlich begrenzte Gültigkeitsdauer von zwei Jahren ab Release-Datum von SafeGuard Enterprise 7.

Hinweis: Wenn Sie eine Aktualisierung von SafeGuard Enterprise 5.6 auf SafeGuard Enterprise 7 durchführen, müssen Sie diese Lizenzdatei manuell in die SafeGuard Enterprise Datenbank importieren

6.3.2 Individuelle Demo-Lizenzdateien

Wenn Sie mehr Lizenzen für die Durchführung einer Evaluierung benötigen als in der Standard-Lizenzdatei enthalten sind, besteht auch die Möglichkeit, eine an Ihre spezifischen Anforderungen angepasste Demo-Lizenz zu erhalten. Wenden Sie sich hierzu bitte an Ihren Vertriebspartner. Diese Art der Demo-Lizenz unterliegt ebenfalls einer zeitlichen Beschränkung. Darüber hinaus ist die Lizenz auf die jeweils mit dem Vertriebspartner vereinbarte Anzahl an Lizenzen pro Modul beschränkt.

Wenn Sie das SafeGuard Management Center starten, werden Sie durch eine Warnungsmeldung darauf aufmerksam gemacht, dass Sie Demo-Lizenzen nutzen. Bei Überschreiten der in einer Demo-Lizenz festgelegten Anzahl an verfügbaren Lizenzen oder der zeitlich begrenzten Nutzungsdauer wird eine Fehlermeldung ausgegeben.

6.4 Lizenzstatusüberblick

So rufen Sie den Lizenzstatusüberblick auf:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den Stammknoten, die Domäne, die OU, das Containerobjekt oder die Arbeitsgruppe.
3. Wechseln Sie im Aktionsbereich in die Registerkarte **Lizenzen**.

Der Lizenzstatus wird angezeigt.

Die Anzeige ist in drei Bereiche unterteilt. Der obere Bereich zeigt den Namen des Kunden, für den die Lizenz ausgestellt wurde, sowie das Datum, an dem die Lizenz ausgestellt wurde.

Der mittlere Bereich liefert detaillierte Informationen zur Lizenz. Die einzelnen Spalten enthalten folgende Angaben:

Spalte	Erklärung
Status (Symbol)	Zeigt den Status der Lizenzen (gültig, Warnung, Fehler) für das jeweilige Modul durch ein Symbol an.
Feature	Zeigt das installierte Modul an.
Erworbene Lizenzen	Zeigt die Anzahl an erworbenen Lizenzen für das installierte Modul an.
Benutzte Lizenzen	Zeigt die Anzahl an genutzten Lizenzen für das installierte Modul an.
Läuft ab	Zeigt das Lizenzablaufdatum an.
Typ	Gibt die Lizenzart, Demo-Lizenz oder reguläre Lizenz, an.
Toleranzwert	Zeigt den festgelegten Toleranzwert für die Überschreitung der Anzahl an erworbenen Lizenzen an.

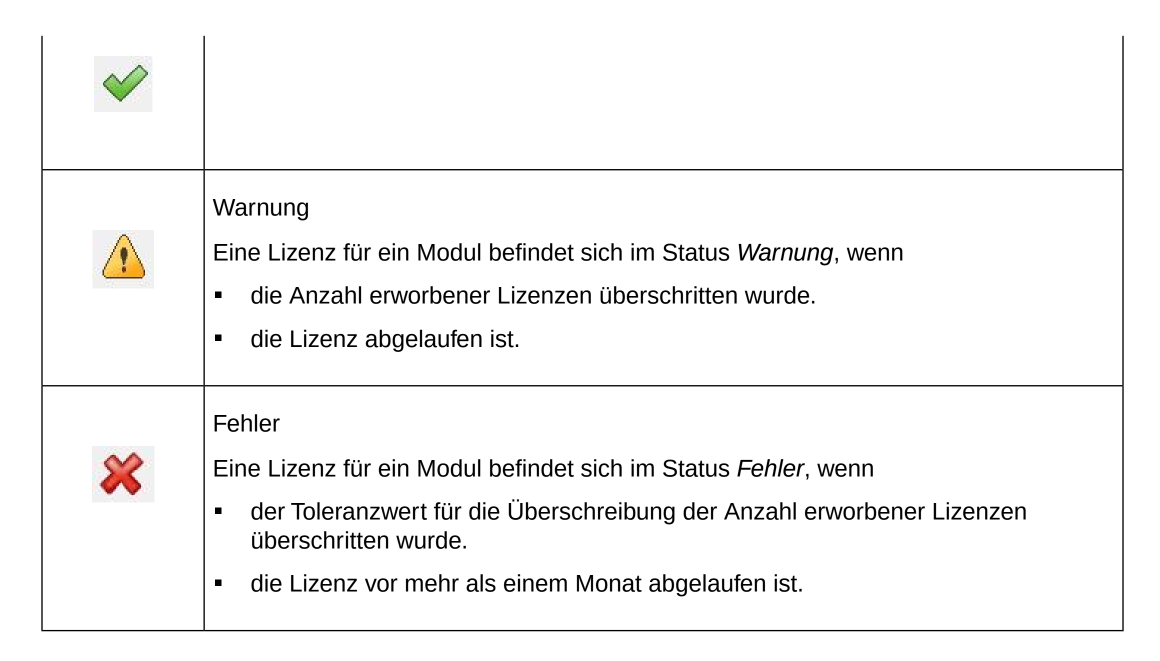
Wenn Sie die Registerkarte **Lizenzen** in einer Domäne/OU aufrufen, zeigt die Übersicht den Status basierend auf den Computern im jeweiligen Zweig.

Unterhalb dieser Übersicht finden Sie Informationen zu den lizenzierten Token-Modulen.

Im unteren Bereich wird der globale Lizenzstatus unabhängig davon, welche Domäne oder OU ausgewählt wurde, angezeigt. Dies erfolgt durch eine Meldung mit einer dem Ampelprinzip folgenden Hintergrundfarbe (Grün = gültig, Gelb = Warnung, Rot = Fehler) und ein Symbol. Bei Warnungs- und Fehlermeldungen erhalten Sie außerdem im unteren Bereich Hinweise zur Aufhebung des ungültigen Lizenzstatus.

Die in der Registerkarte **Lizenzen** angezeigten Symbole haben folgende Bedeutung:

	Gültige Lizenz



✔	
⚠	Warnung Eine Lizenz für ein Modul befindet sich im Status *Warnung*, wenn ▪ die Anzahl erworbener Lizenzen überschritten wurde. ▪ die Lizenz abgelaufen ist.
✖	Fehler Eine Lizenz für ein Modul befindet sich im Status *Fehler*, wenn ▪ der Toleranzwert für die Überschreibung der Anzahl erworbener Lizenzen überschritten wurde. ▪ die Lizenz vor mehr als einem Monat abgelaufen ist.

Sie können die Ansicht des Lizenzstatusüberblicks aktualisieren, indem Sie auf die Schaltfläche **Lizenzstatus aktualisieren** klicken.

6.5 Import von Lizenzdateien

Voraussetzung: Zum Import einer Lizenzdatei in die SafeGuard Enterprise Datenbank benötigt ein Sicherheitsbeauftragter das Recht "Lizenzdatei importieren".

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den Stamm-Knoten, die Domäne oder die OU.
3. Wechseln Sie im Aktionsbereich in die Registerkarte **Lizenzen**.
4. Klicken Sie auf die Schaltfläche **Lizenzdatei importieren**.

   Es wird ein Fenster zur Auswahl der Lizenzdatei angezeigt.

5. Wählen Sie die zu importierende Lizenzdatei aus und klicken Sie auf **Öffnen**.

   Der **Lizenz anwenden?** Dialog mit dem Inhalt der Lizenzdatei wird angezeigt.

6. Klicken Sie auf die Schaltfläche **Lizenz anwenden**.

Die Lizenzdatei wird in die SafeGuard Enterprise Datenbank importiert.

Nach dem Import der Lizenzdatei wird bei Modulen, für die Lizenzen erworben wurden, der Lizenztyp **regulär** angegeben. Bei Modulen, für die keine Lizenzen erworben wurden und für die die Evaluierungslizenz (Standard-Lizenzdatei) oder individuelle Demo-Lizenzen genutzt werden, wird der Lizenztyp **Demo** angegeben.

Hinweis: Wenn Sie eine neue Lizenzdatei importieren, werden jeweils nur die Module, die in dieser Datei enthalten sind, aktualisiert. Alle übrigen Modul-Lizenzinformationen werden entsprechend den in der Datenbank enthaltenen Informationen beibehalten. Diese Importfunktionalität vereinfacht die Evaluierung von zusätzlichen Modulen nach dem Kauf.

6.6 Lizenzüberschreitung

In Ihrer Lizenzdatei ist ein Toleranzwert für die Überschreitung der erworbenen Lizenzen sowie der Lizenzgültigkeitsdauer festgelegt. Bei Überschreiten der verfügbaren Lizenzen pro Modul oder der Gültigkeitsdauer wird somit zunächst eine Warnungsmeldung ausgegeben. Der laufende Betrieb des Systems wird dadurch nicht beeinträchtigt und es tritt in diesem Fall auch keine Einschränkung der Funktionalität in Kraft. So haben Sie die Gelegenheit, den Lizenzstatus zu prüfen und Ihre Lizenz zu erweitern bzw. zu erneuern. Der Toleranzwert ist auf 10 % der Anzahl an erworbenen Lizenzen (der Mindestwert: 5, der Höchstwert: 5.000) festgelegt.

Bei Überschreiten der Toleranzwerte wird eine Fehlermeldung ausgegeben. In diesem Fall tritt eine Funktionalitätseinschränkung in Kraft. Die Übertragung von Richtlinien auf die Endpoints wird deaktiviert. Diese Deaktivierung lässt sich nicht im SafeGuard Management Center manuell wieder aufheben. Die Lizenz muss erweitert bzw. erneuert werden, um wieder alle Funktionen nutzen zu können. Außer der Deaktivierung der Richtlinienübertragung hat die Funktionalitätseinschränkung keine Auswirkungen auf die Endpoints. Bereits zugeordnete Richtlinien bleiben aktiv. Die Deinstallation von Clients ist auch weiterhin möglich.

Die folgenden Abschnitte beschreiben das Systemverhalten bei Lizenzüberschreitungen sowie die Maßnahmen zur Aufhebung der Funktionalitätseinschränkung.

6.6.1 Ungültige Lizenz: Warnung

Ist die Anzahl an verfügbaren Lizenzen überschritten, so wird beim Starten des SafeGuard Management Center eine Warnungsmeldung angezeigt.

Das SafeGuard Management Center wird geöffnet und zeigt den Lizenzstatusüberblick in der Registerkarte **Lizenzen** des Bereichs **Benutzer & Computer**.

Auch hier informiert Sie eine Warnungsmeldung darüber, dass die Lizenz ungültig ist. Über die detaillierten Informationen zur Lizenzdatei lässt sich ermitteln, für welches Modul die Anzahl an verfügbaren Lizenzen überschritten wurde. Durch Verlängerung, Erneuerung oder Erweiterung der Lizenz lässt sich dieser Lizenzstatus ändern.

6.6.2 Ungültige Lizenz: Fehler

Wird der in der Lizenz festgelegte Toleranzwert für die Anzahl an Lizenzen oder die Gültigkeitsdauer überschritten, so zeigt das SafeGuard Management Center eine Fehlermeldung an.

Im SafeGuard Management Center wird die Übertragung von Richtlinien auf die Endpoint-Computer deaktiviert.

In der Registerkarte **Lizenzen** im Bereich **Benutzer & Computer** wird eine Fehlermeldung angezeigt.

Über die detaillierten Informationen zur Lizenzdatei lässt sich ermitteln, für welches Modul die Anzahl an verfügbaren Lizenzen überschritten wurde.

Um die Einschränkung der Funktionalität aufzuheben, habe Sie folgende Möglichkeiten:

- Lizenzen umverteilen

  Um ausreichend verfügbare Lizenzen zu erhalten, können Sie die Software auf nicht genutzten Endpoints deinstallieren und diese somit dauerhaft aus der SafeGuard Enterprise Datenbank entfernen.

- Lizenzen erweitern/erneuern

  Wenden Sie sich an Ihren Vertriebspartner, um Ihre Lizenz zu erweitern bzw. zu erneuern. Sie erhalten eine neue Lizenzdatei zum Import in die SafeGuard Enterprise Datenbank.

- Neue Lizenzdatei importieren

  Wenn Sie Ihre Lizenz bereits erneuert bzw. erweitert haben, importieren Sie die erhaltene Lizenzdatei in die SafeGuard Enterprise Datenbank. Diese neu importierte Datei ersetzt die ungültige Lizenzdatei.

Durch Umverteilen von Lizenzen oder Importieren einer gültigen Lizenzdatei wird die Funktionalitätseinschränkung aufgehoben und der normale Betrieb des Systems kann fortgesetzt werden.

7 Mit mehreren Datenbankkonfigurationen arbeiten

Das SafeGuard Management Center ermöglicht die Benutzung mehrerer Datenbankkonfigurationen (Multi Tenants). Wenn Sie diese Funktion nutzen möchten, müssen Sie sie während der Installation aktivieren. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

Mit Multi Tenancy können Sie verschiedene SafeGuard Enterprise Datenbankkonfigurationen konfigurieren und sie für eine Instanz des SafeGuard Management Centers verwalten. Dies erweist sich vor allem dann als nützlich, wenn Sie verschiedene Konfigurationen für verschiedene Domänen, OUs oder Unternehmensstandorte einsetzen möchten.

Voraussetzung: Die Funktion Multi Tenancy muss über eine Installation vom Typ **Vollständig** installiert worden sein. Die initiale Konfiguration des SafeGuard Management Center muss durchgeführt worden sein.

Um die Konfigurationsarbeiten zu erleichtern, haben Sie folgende Möglichkeiten:

- Mehrere Datenbankkonfigurationen erstellen.
- Zuvor erstellte Datenbankkonfiguration auswählen.
- Datenbankkonfiguration löschen.
- Zuvor erstellte Datenbankkonfiguration aus einer Datei importieren.
- Datenbankkonfiguration zur späteren Wiederverwendung exportieren.

7.1 Erstellen von weiteren Datenbankkonfigurationen

So erstellen Sie eine weitere SafeGuard Enterprise Datenbankkonfiguration nach der Erstkonfiguration:

1. Starten Sie das SafeGuard Management Center.

   Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Klicken Sie auf **Neu**.

   Der SafeGuard Management Center Konfigurationsassistent wird automatisch gestartet. Der Assistent führt Sie durch die notwendigen Schritte für das Anlegen einer neuen Datenbankkonfiguration.

3. Nehmen Sie die erforderlichen Einstellungen vor.

   Die neue Datenbankkonfiguration wird erstellt.

4. Zur Anmeldung an das SafeGuard Management Center werden Sie dazu aufgefordert, den Namen des Sicherheitsbeauftragten für diese Konfiguration auszuwählen und Ihr Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der neuen Datenbankkonfiguration verbunden. Wenn Sie das SafeGuard Management Center das nächste Mal starten, können Sie die neue Datenbank-Konfiguration aus der Liste auswählen.

7.2 Herstellen einer Verbindung mit einer bereits vorhandenen Datenbankkonfiguration

So benutzen Sie eine bereits vorhandene SafeGuard Enterprise Datenbankkonfiguration:

1. Starten Sie das SafeGuard Management Center.

   Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Wählen Sie die Datenbankkonfiguration, die Sie verwenden möchten, aus der Dropdownliste und klicken Sie auf **OK**.

   Die ausgewählte Datenbankkonfiguration wird mit dem SafeGuard Management Center verbunden und wird aktiv.

3. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der ausgewählten Datenbankkonfiguration verbunden.

7.3 Export einer Konfiguration in eine Datei

Um eine Konfiguration zu speichern, damit sie später wiederverwendet werden kann, können Sie sie in eine Datei exportieren.

1. Starten Sie das SafeGuard Management Center.

   Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Wählen Sie die gewünschte Konfiguration aus der Liste und klicken Sie auf **Exportieren...**
3. Zum Schutz der Konfigurationsdatei werden Sie dazu aufgefordert, ein Kennwort, das die Konfigurationsdatei verschlüsselt, einzugeben und zu bestätigen. Klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die exportierte Konfigurationsdatei *.SGNConfig an.

   Sollte diese Konfiguration bereits vorhanden sein, so werden Sie gefragt, ob Sie die vorhandene Konfiguration überschreiben möchten.

Die Datenbankkonfiguration wird am angegebenen Speicherort gespeichert.

7.4 Import einer Konfiguration aus einer Datei

Um eine Datenbankkonfiguration zu verwenden oder zu ändern, können Sie eine zuvor erstellte Konfiguration in das SafeGuard Management Center importieren. Hier gibt es zwei Möglichkeiten:

- über das SafeGuard Management Center (für Multi Tenancy)
- durch Doppelklicken auf die Konfigurationsdatei (für Single und Multi Tenancy)

7.5 Import einer Konfiguration über das SafeGuard Management Center

1. Starten Sie das SafeGuard Management Center.

   Der Dialog **Konfiguration auswählen** wird angezeigt.

2. Klicken Sie auf **Import...**, wählen Sie die gewünschte Konfigurationsdatei aus und klicken Sie auf **Öffnen**.
3. Geben Sie das Kennwort ein, das während des Exports für die Konfigurationsdatei erstellt wurde, und klicken Sie auf **OK**.

   Die ausgewählte Konfiguration wird angezeigt.

4. Um die Konfiguration zu aktivieren, klicken Sie auf **OK**.
5. Zur Authentisierung werden Sie dazu aufgefordert, den Sicherheitsbeauftragtennamen für diese Konfiguration auszuwählen und das entsprechende Zertifikatsspeicherkennwort einzugeben. Klicken Sie auf **OK**.

Das SafeGuard Management Center wird geöffnet und mit der importierten Datenbankkonfiguration verbunden.

7.6 Import einer Konfiguration durch Doppelklicken auf die Konfigurationsdatei (Single und Multi Tenancy)

Hinweis: Dieser Vorgang ist sowohl im Single Tenancy als auch im Multi Tenancy Modus möglich.

Es besteht auch die Möglichkeit, eine Konfiguration zu exportieren und diese an mehrere Sicherheitsbeauftragte zu verteilen. Die Sicherheitsbeauftragten müssen lediglich auf die Konfigurationsdatei doppelklicken, um ein vollständig konfiguriertes SafeGuard Management Center zu öffnen.

Dies erweist sich vor allem dann als vorteilhaft, wenn Sie die SQL Authentisierung für die Datenbank verwenden und vermeiden möchten, dass das SQL-Kennwort jedem Administrator bekannt ist. Sie müssen das Kennwort dann nur einmal eingeben, eine Konfigurationsdatei erstellen und sie an die Computer der Sicherheitsbeauftragten verteilen.

Voraussetzung: Die Erstkonfiguration des SafeGuard Management Centers muss durchgeführt worden sein. Detaillierte Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

1. Starten Sie das SafeGuard Management Center.
2. Wählen Sie im **Extras** Menü **Optionen** und wechseln Sie in die Registerkarte **Datenbank**.
3. Geben Sie die Anmeldeinformationen für die SQL Datenbankserververbindung ein oder bestätigen Sie diese.
4. Klicken Sie auf **Konfiguration exportieren**, um die Konfiguration in eine Datei zu exportieren.
5. Geben Sie ein Kennwort für die Konfigurationsdatei ein und bestätigen Sie es.
6. Geben Sie einen Dateinamen ein und wählen Sie einen Speicherort aus.
7. Verteilen Sie die Konfigurationsdatei an die Computer der Sicherheitsbeauftragten. Teilen Sie ihnen das Kennwort für diese Datei sowie das Zertifikatsspeicherkennwort mit, das Sie für Anmeldung an das SafeGuard Management Center benötigen.

8. Die Sicherheitsbeauftragten müssen nur auf die Konfigurationsdatei doppelklicken.
9. Sie werden aufgefordert, das Kennwort für die Konfigurationsdatei einzugeben.
10. Zur Anmeldung an das SafeGuard Management Center werden die Sicherheitsbeauftragten aufgefordert, ihr Zertifikatsspeicherkennwort einzugeben.

Das SafeGuard Management Center startet mit der importierten Konfiguration. Diese Konfiguration ist die neue Standardkonfiguration.

7.7 Schneller Wechsel zwischen Datenbankkonfigurationen

Zur Vereinfachung von Verwaltungsaufgaben bei mehreren Datenbanken bietet das SafeGuard Management Center den schnellen Wechsel zwischen Datenbankkonfigurationen.

Hinweis: Dieser Vorgang ist auch im Single Tenancy Modus möglich.

1. Wählen Sie **Datei** in der Menüleiste des SafeGuard Management Centers und klicken Sie auf **Konfiguration wechseln...**
2. Wählen Sie die Datenbank, zu der Sie wechseln möchten, aus der Dropdownliste aus und klicken Sie auf **OK**.

Das SafeGuard Management Center wird automatisch mit der ausgewählten Konfiguration neu gestartet.

7.8 Prüfen der Datenbankintegrität

Bei der Anmeldung an die Datenbank wird die Datenbankintegrität automatisch geprüft. Sollte diese Überprüfung Fehler ergeben, wird der Dialog **Datenbankintegrität prüfen** angezeigt.

Sie können die Datenbankintegrität auch jederzeit nach der Anmeldung prüfen und hierzu den Dialog **Datenbankintegrität prüfen** aufrufen:

1. Wählen Sie in der Menüleiste des SafeGuard Management Center **Extras > Datenbankintegrität**.
2. Um die Tabellen zu prüfen, klicken Sie auf **Alle prüfen** oder **Ausgewählte prüfen**.

Danach werden fehlerhafte Tabellen im Dialog markiert. Um die Fehler zu beheben, klicken Sie auf **Reparieren**.

Hinweis: Nach einer Aktualisierung des SafeGuard Enterprise Backend (SQL) wird die Prüfung der Datenbankintegrität immer gestartet. Die Prüfung muss einmal pro SafeGuard Enterprise Datenbank durchgeführt werden, um die Aktualisierung abzuschließen.

8 Registrieren und Konfigurieren des SafeGuard Enterprise Server

Zur Implementierung der Informationen für die Kommunikation zwischen IIS Server, Datenbank und dem SafeGuard-geschützten Endpoint muss der SafeGuard Enterprise Server registriert und konfiguriert werden. Die Informationen werden in einem Server-Konfigurationspaket gespeichert.

Diesen Schritt führen Sie im SafeGuard Management Center durch. Der Workflow ist davon abhängig, ob der SafeGuard Enterprise Server auf demselben Computer wie das SafeGuard Management Center oder auf einem anderen Computer installiert ist.

Sie können auch weitere Eigenschaften festlegen. So lassen sich z. B. zusätzliche Sicherheitsbeauftragte für den ausgewählten Server hinzufügen. Sie können auch die Verbindung zur Datenbank konfigurieren.

8.1 Registrieren und Konfigurieren des SafeGuard Enterprise Server für den aktuellen Computer

Wenn Sie das SafeGuard Management Center und SafeGuard Enterprise Server auf dem Computer, mit dem Sie derzeit arbeiten, installiert haben, registrieren und konfigurieren Sie den SafeGuard Enterprise Server.

Hinweis:

Wenn Multi Tenancy installiert ist, steht diese Option nicht zur Verfügung.

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server** und klicken Sie auf **Diesen Computer zum SGN Server machen**.
4. Wählen Sie die Registerkarte **Server** und klicken Sie auf **Optionen**:

   Das SafeGuard Enterprise Server Configuration Setup wird automatisch gestartet.

5. Übernehmen Sie in allen folgenden Dialogen die Standardeinstellungen.

Der SafeGuard Enterprise Server ist installiert. Ein Server-Konfigurationspaket mit der Bezeichnung **`<Server>.msi`** wird erstellt und direkt auf dem aktuellen Computer installiert. Die Serverinformationen werden in der Registerkarte **Server** angezeigt. Sie können zusätzliche Konfigurationsschritte durchführen.

Hinweis: Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das alte Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.2 Registrieren und Konfigurieren des SafeGuard Enterprise Servers für einen anderen Computer

Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert wurde, registrieren und konfigurieren Sie den SafeGuard Enterprise Server:

1. Starten Sie das SafeGuard Management Center.
2. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
3. Wählen Sie die Registerkarte **Server** und klicken Sie auf **Hinzufügen**.
4. Klicken Sie unter **Serverregistrierung** auf die Schaltfläche **[...]**, um das Maschinenzertifikat des Servers auszuwählen. Es wird bei der Installation des SafeGuard Enterprise Servers erzeugt. Sie finden es standardmäßig im Verzeichnis `MachCert` des SafeGuard Enterprise Server Installationsverzeichnisses. Es trägt den Dateinamen `<Computername>.cer`. Wenn der SafeGuard Enterprise Server auf einem anderen Computer als das SafeGuard Management Center installiert ist, muss diese .cer-Datei als Kopie oder Netzwerkfreigabe zugreifbar sein.

   Wählen Sie nicht das MSO-Zertifikat.

   Der Fully Qualified Name (FQDN), z. B. `server.mycompany.com`, sowie Zertifikatsinformationen werden angezeigt.

   Hinweis:

   Wenn Sie einen Mac Endpoint zu einem SGN Server verbinden, müssen Sie **SSL** in der Spalte **Transportverschlüsselung** wählen, um die Verbindung abzusichern.

   Wenn SSL als Transportverschlüsselung zwischen Endpoint und Server verwendet werden soll, muss der Servername, den Sie hier eingeben, mit dem Servernamen übereinstimmen, den Sie im SSL-Zertifikat vergeben haben. Andernfalls ist keine Kommunikation möglich.

   Wenn Sie die Verbindung konfigurieren, stellen Sie sicher, HTTPS-Portnummer 443 zu öffnen.

5. Klicken Sie auf **OK**.

   Die Serverinformationen werden in der Registerkarte **Server** angezeigt.

6. Klicken Sie auf die Registerkarte **Server-Pakete**. Hier werden alle verfügbaren Server angezeigt. Wählen Sie dort den gewünschten Server aus. Geben Sie einen Ausgabepfad für das Konfigurationspaket an. Klicken Sie auf **Konfigurationspaket erstellen**.

   Ein Server-Konfigurationspaket (MSI) mit der Bezeichnung `<Server>.msi` wird im angegebenen Ausgabeort erstellt.

7. Bestätigen Sie die Erfolgsmeldung mit **OK**.
8. Klicken Sie in der Registerkarte **Server** auf **Schließen**.

Die Registrierung und Konfiguration des SafeGuard Enterprise Servers ist beendet. Installieren Sie das Server-Konfigurationspaket (MSI) auf dem Computer, auf dem der SafeGuard Enterprise Server läuft. Sie können die Serverkonfiguration in der Registerkarte **Server** jederzeit ändern.

Hinweis: Wenn Sie ein neues Server-Konfigurationspaket (MSI) auf dem SafeGuard Enterprise Server installieren möchten, deinstallieren Sie zunächst das alte Konfigurationspaket. Löschen Sie darüber hinaus den Local Cache manuell, so dass er mit den neuen Konfigurationsdaten (z. B. SSL-Einstellungen) aktualisiert werden kann. Installieren Sie dieses Konfigurationspaket auf dem Server.

8.3 Ändern der SafeGuard Enterprise Server Eigenschaften

Sie können die Eigenschaften und Einstellungen für jeden registrierten Server und seine Datenbankverbindung jederzeit ändern.

1. Wählen Sie den gewünschten Server in der Registerkarte **Server** des SafeGuard Management Center **Konfigurationspakete** Werkzeugs.
2. Gehen Sie wie folgt vor:

Element	Beschreibung
Skript ausführen	Klicken Sie hier, um die Verwendung von SafeGuard Enterprise Management API zu ermöglichen. Dies ermöglicht die Ausführung von administrativen Aufgaben über Skripte
Server-Rollen	Klicken Sie hier, um eine verfügbare Sicherheitsbeauftragtenrolle für den ausgewählten Server zu aktivieren/deaktivieren.
Win. Auth. WHD	Dieses Kontrollkästchen muss für die Windows Authentisierung zu SafeGuard Web Helpdesk am ausgewählten Server markiert sein. Wenn das Kontrollkästchen nicht gesetzt ist, haben nur Sicherheitsbeauftragte mit den entsprechenden Web Helpdesk-Rechten Zugang zu Web Helpdesk. Nähere Informationen zur Windows Authentisierung zu SafeGuard Web Helpdesk finden Sie im *SafeGuard Web Helpdesk* Handbuch.
Server-Rolle hinzufügen...	Klicken Sie hier, um weitere spezifische Sicherheitsbeauftragtenrollen für den ausgewählten Server hinzuzufügen, falls erforderlich. Sie werden dazu aufgefordert, das Serverzertifikat auszuwählen. Die Sicherheitsbeauftragtenrolle wird hinzugefügt und kann unter **Server-Rollen** angezeigt werden.
Datenbankverbindung	Klicken Sie auf **[...]**, um die Verbindung zur Datenbank für jeden registrierten Server zu konfigurieren. Hier können Sie auch die Anmeldeinformationen für die Datenbank und die Transportverschlüsselung zwischen Web Server und Datenbankserver festlegen. Weitere Informationen finden Sie unter Konfigurieren der Datenbankserververbindung (Seite 20). Selbst wenn die Prüfung der Datenbankverbindung nicht erfolgreich ist, kann ein neues Server-Konfigurationspaket erstellt werden. **Hinweis:** Sie müssen nicht den SafeGuard Management Center Konfigurationsassistenten erneut ausführen, um die Datenbankkonfiguration zu aktualisieren. Erstellen Sie einfach ein neues Server-Konfigurationspaket und verteilen Sie es an den entsprechenden Server. Sobald dieses auf dem Server installiert ist, kann auf die neue Datenbankverbindung zugegriffen werden.

3. Erstellen Sie ein neues Server-Konfigurationspaket in der Registerkarte **Server-Pakete**.

4. Deinstallieren Sie das alte Server-Konfigurationspaket und installieren Sie danach das neue auf dem entsprechenden Server.

Die neue Server-Konfiguration wird aktiv.

8.4 Registrieren des SafeGuard Enterprise Servers mit aktivierter Sophos Firewall

Ein durch SafeGuard Enterprise geschützter Endpoint kann keine Verbindung mit dem SafeGuard Enterprise Server herstellen, wenn eine Sophos Firewall mit Standardeinstellungen auf dem Endpoint installiert ist. Die Sophos Firewall sperrt standardmäßig NetBIOS-Verbindungen, die für die Auflösung des Netzwerknamens des SafeGuard Enterprise Servers benötigt werden.

1. Führen Sie als Workaround einen der folgenden Schritte aus:
   - Geben Sie die NetBIOS-Verbindungen in der Firewall frei.
   - Fügen Sie den Fully Qualified Name des SafeGuard Enterprise Servers im Konfigurationspaket hinzu. Weitere Informationen finden Sie unter Registrieren und Konfigurieren des SafeGuard Enterprise Server für einen anderen Computer (Seite 38).

9 Sichern von Transportverbindungen mit SSL

SafeGuard Enterprise unterstützt zur Erhöhung der Sicherheit die Verschlüsselung der Transportverbindungen zwischen den einzelnen Komponenten mit SSL.

- Die Verbindung zwischen dem Datenbankserver und dem Web Server sowie die Verbindung zwischen dem Datenbankserver und dem Computer, auf dem das SafeGuard Management Center installiert ist, kann mit SSL verschlüsselt werden.

- Die Verbindung zwischen dem SafeGuard Enterprise Server und dem von SafeGuard Enterprise verwalteten Computer kann entweder mit SSL oder mit SafeGuard-spezifischer Verschlüsselung verschlüsselt werden. Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und daher eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung.

  Mac: Um die Verbindung zwischen dem SafeGuard Enterprise Server und Mac Endpoints abzusichern, muss SSL verwendet werden.

  Hinweis: Wir empfehlen dringend, SSL-verschlüsselte Kommunikation zu verwenden, es sei denn, es handelt sich um Demo- oder Test-Installationen. Falls dies nicht möglich ist und die SafeGuard-spezifische Verschlüsselung verwendet wird, so gilt die Obergrenze von 1000 Clients, die eine Verbindung mit einer Serverinstanz herstellen können.

Bevor SSL für SafeGuard Enterprise aktiviert werden kann, muss eine funktionsfähige SSL-Umgebung eingerichtet werden.

Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

9.1 Einrichten von SSL

Die folgenden allgemeinen Aufgaben müssen für die SSL-Einrichtung auf dem Web Server durchgeführt werden:

- Certificate Authority muss auf dem Server installiert sein, um die bei der SSL-Verschlüsselung verwendeten Zertifikate auszustellen.

- Ein Zertifikat muss ausgestellt und der IIS Server so konfiguriert werden, dass er SSL verwendet und auf das Zertifikat zeigt.

- Der Servername, den Sie bei der Konfiguration des SafeGuard Enterprise Servers angeben, muss identisch sein mit dem Servernamen, den Sie vorab im SSL-Zertifikat angegeben haben. Sonst können Client und Server nicht miteinander kommunizieren. Für jeden SafeGuard Enterprise Server wird ein separates SSL-Zertifikat benötigt.

- Wenn Sie Network Load Balancer einsetzen, vergewissern Sie sich, dass der Portbereich den SSL-Port mit einschließt.

Weitere Informationen erhalten Sie von unserem technischen Support oder hier:

- http://msdn2.microsoft.com/en-us/library/ms998300.aspx

- http://support.microsoft.com/default.aspx?scid=kb;de-de;316898

- https://blogs.msdn.com/sql_protocols/archive/2005/11/10/491563.aspx

Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

9.2 Aktivieren der SSL-Verschlüsselung in SafeGuard Enterprise

So aktivieren Sie die SSL-Verschlüsselung in SafeGuard Enterprise:

- Verbindung zwischen Web Server und Datenbankserver:

  Aktivieren Sie SSL-Verschlüsselung während der Registrierung des SafeGuard Enterprise Servers im SafeGuard Management Center Konfigurationspakete-Werkzeug. Weitere Informationen finden Sie unter Konfigurieren der Datenbankserververbindung (Seite 20) oder unter: http://www.sophos.com/de-de/support/knowledgebase/109012.aspx.

- Für die Verbindung zwischen Datenbankserver und SafeGuard Management Center

  Aktivieren Sie die SSL-Verschlüsselung im SafeGuard Management Center Konfigurationsassistenten (siehe Konfigurieren der Datenbankserververbindung (Seite 20)).

- Verbindung zwischen SafeGuard Enterprise Server und durch SafeGuard Enterprise geschützte Endpoints:

  Aktivieren Sie die SSL-Verschlüsselung beim Erzeugen des Konfigurationspakets für den durch SafeGuard Enterprise verwalteten Endpoint im SafeGuard Management Center Konfigurationspakete-Werkzeug (siehe Erstellen eines Konfigurationspakets für verwaltete Endpoints (Seite 101)). Nähere Informationen, wie SSL am SafeGuard Enterprise Server und dem durch SafeGuard Enterprise geschützten Endpoint zu konfigurieren ist, entnehmen sie der *SafeGuard Enterprise Installationsanleitung*.

Sie können die SSL-Verschlüsselung für SafeGuard Enterprise während der Erstkonfiguration der SafeGuard Enterprise Komponenten oder zu einem späteren Zeitpunkt einrichten. Erstellen Sie danach ein neues Konfigurationspaket und installieren Sie es auf dem entsprechenden Server oder zentral verwalteten Computer.

Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

10 Aufbau der Organisationsstruktur

Für den Aufbau einer Organisationsstruktur im SafeGuard Management Center gibt es zwei Möglichkeiten:

- Sie können eine bestehende Organisationsstruktur über ein Active Directory in die SafeGuard Enterprise Datenbank importieren.
- Sie können Ihre Organisationsstruktur manuell anlegen, indem Sie Arbeitsgruppen und Domänen sowie eine Struktur für die Verwaltung von Richtlinien erstellen.

10.1 Import aus Active Directory

Sie können eine bestehende Organisationsstruktur über ein Active Directory in die SafeGuard Enterprise Datenbank importieren.

Wir empfehlen, ein spezielles Windows-Servicekonto anzulegen, das für alle Import- und Synchronisierungsaufgaben verwendet wird. So stellen Sie sicher, dass alle Import-Vorgänge korrekt durchgeführt werden und verhindern, dass Objekte in der SafeGuard Enterprise Datenbank unbeabsichtigt gelöscht werden. Für Informationen zum Zuweisen der notwendigen Rechte, siehe http://www.sophos.com/de-de/support/knowledgebase/107979.aspx.

10.1.1 Importieren der Organisationsstruktur

Hinweis: Mit dem SafeGuard Management Center Taskplaner können Sie einen periodischen Task für die automatische Synchronisierung zwischen dem Active Directory und SafeGuard Enterprise erstellen. In Ihrer Produktlieferung steht hierzu eine vordefinierte Skript-Vorlage zur Verfügung. Weitere Informationen finden Sie unter Planung von Tasks (Seite 283) und Vordefinierte Skripte für regelmäßig wiederkehrende Tasks (Seite 289).

1. Wählen Sie im SafeGuard Management Center **Extras > Optionen**.
2. Wählen Sie die Registerkarte **Verzeichnis** und klicken Sie auf **Hinzufügen**.
3. Gehen Sie in **LDAP Authentisierung** folgendermaßen vor:

   a) Bei **Servername oder IP** geben Sie den NetBIOS-Name des Domänencontrollers oder dessen IP ein.

   b) Bei **Anmeldeinformationen des Benutzers** geben Sie Ihre Windows-Anmeldeinformationen zur Umgebung ein.

   c) Klicken Sie auf **OK**.

   Hinweis: Bei Windows Einzelplatzcomputern muss auf dem Computer ein Verzeichnis freigegeben sein, damit eine Verbindung via LDAP möglich wird.

4. Klicken Sie auf **Benutzer & Computer**.
5. Klicken Sie im linken Navigationsfenster auf das Stammverzeichnis **Stamm [Filter ist aktiv]**.
6. Klicken Sie im Aktionsbereich auf der rechten Seite auf die Registerkarte **Synchronisieren**.
7. Wählen Sie das gewünschte Verzeichnis aus der **Verzeichnis DSN** Liste und klicken Sie auf das Lupensymbol (oben rechts).

   Es erscheint eine Abbildung der Active Directory-Struktur der Organisationseinheiten (OU) in Ihrem Unternehmen.

8. Markieren Sie die Organisationseinheiten (OU), die synchronisiert werden sollen. Es muss nicht der gesamte Inhalt des Active Directory importiert werden.
9. Um auch Mitgliedschaften zu synchronisieren, wählen Sie das Kontrollkästchen **Synchronisiere Mitgliedschaften**. Um auch den Benutzer Aktiv-Status zu synchronisieren, wählen Sie das Kontrollkästchen **Synchronisiere Benutzer Aktiv-Status**.
10. Klicken Sie unten im Aktionsbereich auf **Synchronisieren**.

    Wenn Sie Benutzer und ihre Gruppenzugehörigkeit synchronisieren, wird die Zugehörigkeit zu einer “Primärgruppe“ nicht synchronisiert, da sie für die Gruppe nicht sichtbar ist.

Die Domänen werden synchronisiert. Details zur Synchronisierung werden angezeigt. Klicken Sie auf die Meldung, die in der Statusleiste unterhalb der Schaltflächen auf der linken Seite angezeigt wird, um ein Synchronisierungsprotokoll einzusehen. Klicken Sie auf das Protokoll, um es in die Zwischenablage zu kopieren und es in eine E-Mail oder eine Datei einzufügen.

Hinweis: Wenn Elemente von einer untergeordneten Baumstruktur in eine andere im Active Directory verschoben wurden, müssen beide Baumstrukturen mit der SQL-Datenbank synchronisiert werden. Wird nur eine untergeordnete Datenbank synchronisiert, so werden die Elemente nicht verschoben, sondern gelöscht.

Hinweis: Es wird empfohlen, Importvorgänge mit mehr als 400.000 Objekten aus dem AD in mehrere Vorgänge aufzuteilen. Unter Umständen ist dies nicht möglich, wenn sich mehr als 400.000 Objekte in einer Organisationseinheit befinden.

10.1.2 Eine neue Domäne aus einem Active Directory importieren

1. Klicken Sie im linken Navigationsfenster auf das Stammverzeichnis **Stamm [Filter ist aktiv]**.
2. Wählen Sie **Datei > Neu > Neue Domäne aus AD importieren**.
3. Klicken Sie im Aktionsbereich auf der rechten Seite auf **Synchronisieren**.
4. Wählen Sie das gewünschte Verzeichnis aus der **Verzeichnis DSN** Liste und klicken Sie auf das Lupensymbol (oben rechts).

    Es erscheint eine Abbildung der Active Directory-Struktur der Organisationseinheiten (OU) in Ihrem Unternehmen.

5. Wählen Sie die Domäne, die synchronisiert werden soll, und klicken Sie auf **Synchronisieren**.

Hinweis: Wenn Elemente von einer untergeordneten Baumstruktur in eine andere im Active Directory verschoben wurden, müssen beide Baumstrukturen mit der SQL-Datenbank synchronisiert werden. Wird nur eine untergeordnete Datenbank synchronisiert, so werden die Elemente nicht verschoben, sondern gelöscht.

Hinweis: Durch die AD-Synchronisierung wird der (NetBIOS)-Name der Domäne vor Windows 2000 nicht synchronisiert, wenn der Domänen-Controller mit einer IP-Adresse konfiguriert ist. Konfigurieren Sie den Domänen-Controller so, dass stattdessen der Servername (NetBIOS oder DNS) verwendet wird. Der Client (auf dem die AD-Synchronisierung läuft) muss entweder Teil der Domäne sein oder es muss sichergestellt sein, dass der DNS-Name zum Ziel-Domänen-Controller aufgelöst werden kann.

10.1.3 Zugriffsrechte für Sicherheitsbeauftragte und Import aus Active Directory

Für die erforderlichen Zugriffsrechte für den Import der Organisationsstruktur aus Active Directory gilt:

- Wenn Sie eine Active Directory Verbindung zu einer bereits vorhandenen Domäne hinzufügen, gilt Folgendes:
  - Wenn Sie das Zugriffsrecht **Voller Zugriff** für die Domäne (DNS) haben, werden die Anmeldeinformationen für die Directory-Verbindung aktualisiert.
  - Wenn Sie das Zugriffsrecht **Schreibgeschützt** oder weniger Zugriffsrechte für die Domäne (DNS) haben, werden die Anmeldeinformationen nicht aktualisiert. Sie können jedoch vorhandene Anmeldeinformationen für die Synchronisierung benutzen.
- Für Active Directory Import und Synchronisierung werden die Zugriffsrechte für einen Container oder eine Domäne auf die Domänenbaumstruktur, die sie importieren können, übertragen. Wenn Sie für eine untergeordnete Baumstruktur nicht das Zugriffsrecht **Voller Zugriff** haben, kann diese nicht synchronisiert werden. Wenn eine untergeordnete Baumstruktur nicht geändert werden kann, wird sie nicht in der Synchronisierungs-Baumstruktur angezeigt.
- Unabhängig von Ihren Sicherheitsbeauftragten-Zugriffsrechten für Verzeichnisobjekte können Sie eine neue Domäne aus dem Active Directory importieren, wenn diese noch nicht in der SafeGuard Enterprise Datenbank existiert. Sie und Ihre übergeordneten Sicherheitsbeauftragten erhalten automatisch das Zugriffsrecht **Voller Zugriff** für die neue Domäne.
- Wenn Sie einen untergeordneten Container (Sub-Container) für die Synchronisierung auswählen, muss die Synchronisierung bis zum Stammverzeichnis durchgeführt werden. In der Synchronisierungs-Baumstruktur werden alle relevanten Container automatisch ausgewählt. Dies ist auch dann der Fall, wenn sich über dem Sub-Container Container befinden, die gemäß ihren Zugriffsrechten **Schreibgeschützt** sind, oder für die der Zugriff **Verweigert** wird. Wenn Sie die Auswahl eines Sub-Containers aufheben, müssen Sie dies entsprechend Ihren Zugriffsrechten auch bei den Containern darüber bis zum Stammverzeichnis tun.

  Wenn eine Gruppe, für die nur die Zugriffsrechte **Schreibgeschützt** oder **Verweigert** verfügbar sind, in den Synchronisierungsvorgang einbezogen wird, passiert Folgendes:
  - Die Gruppenmitgliedschaften werden nicht aktualisiert.
  - Wenn die Gruppe im Active Directory gelöscht wurde, wird sie nicht aus der SafeGuard Enterprise Datenbank gelöscht.
  - Wenn die Gruppe jedoch im Active Directory verschoben wurde, wird sie auch innerhalb der SafeGuard Enterprise Struktur verschoben. Dies ist auch dann der Fall, wenn sie in einen Container verschoben werden soll, für den Sie nicht das **Voller Zugriff** Zugriffsrecht haben.

  Wenn ein Container mit den Zugriffsrechten **Schreibgeschützt** oder **Verweigert** zur Synchronisierung hinzugefügt wird, da er sich auf dem Weg zum Stammverzeichnis befindet, und dieser Container eine Gruppe mit dem Zugriff **Voller Zugriff** enthält, wird diese Gruppe synchronisiert. Gruppen mit den Zugriffsrechten **Schreibgeschützt** oder **Verweigert** werden nicht synchronisiert.

10.2 Erstellen von Arbeitsgruppen und Domänen

Sicherheitsbeauftragte mit den erforderlichen Berechtigungen können manuell Arbeitsgruppen oder Domänen mit einer Struktur für die Verwaltung von Richtlinien anlegen. Auch die Zuweisung von Richtlinien und/oder Verschlüsselungsregeln an lokale Benutzer ist dadurch möglich.

Sie müssen Domänen nur dann manuell anlegen, wenn Sie keine Domänen aus dem Active Directory (AD) importieren wollen oder können, z. B. weil kein AD vorhanden ist.

10.2.1 Registrierung als neuer Benutzer

Informationen zu Benutzern, die sich zum ersten Mal bei SafeGuard Enterprise anmelden, finden Sie unter SafeGuard Enterprise Power-on Authentication (POA) (Seite 104).

Wenn sich ein neuer Benutzer an SafeGuard Enterprise anmeldet, wird dieser sobald der Endpoint eine Verbindung mit dem SafeGuard Enterprise Server hergestellt hat, registriert und in im Bereich **Benutzer und Computer** des SafeGuard Management Center unter der entsprechenden Domäne oder Arbeitsgruppe angezeigt.

Das für diese Benutzer/Computer vorgesehene Verzeichnis **.Automatisch registriert** wird automatisch unterhalb des Stammverzeichnisses sowie unter jeder Domäne/Arbeitsgruppe erzeugt. Es kann nicht umbenannt oder verschoben werden. Objekte in diesem Verzeichnis können auch nicht manuell verschoben werden. Wenn die Organisationseinheit (Organizational Unit, OU) beim nächsten Kontakt mit der SafeGuard Enterprise Datenbank synchronisiert wird, wird das Objekt in die entsprechenden OU verschoben. Andernfalls verbleibt Sie im Verzeichnis **.Automatisch registriert** der jeweiligen Domäne/Arbeitsgruppe.

Als Sicherheitsbeauftragter können Sie dann die automatisch registrierten Objekte wie üblich verwalten.

Hinweis: Lokale Benutzer können sich nicht mit einem leeren Kennwort an SafeGuard Enterprise anmelden. Wenn sich lokale Benutzer mit leerem Kennwort an SafeGuard Enterprise anmelden, bleiben sie Gastbenutzer und werden nicht in der Datenbank gespeichert. Wenn für diese Benutzer zudem noch Windows Autologon aktiviert ist, wird die Anmeldung abgebrochen. Für die erfolgreiche Anmeldung an SafeGuard Enterprise muss in diesem Fall ein neues Kennwort vergeben werden und das Autologon für Windows in der Registry des Endpoint deaktiviert werden.

Hinweis: Microsoft Konten werden immer als SafeGuard Enterprise Gastbenutzer behandelt.

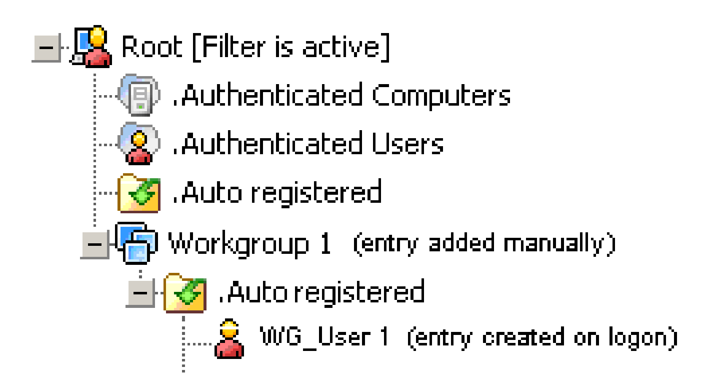
10.2.2 Beispiele für die automatische Registrierung

Im Folgenden finden Sie zwei Beispiele für das Verhalten von automatisch registrierten Objekten.

Benutzer/Computer außerhalb eines Active Directory

In einem Unternehmen müssen nicht zwangsläufig alle Benutzer/Computer Teil eines Active Directory (AD) sein, z. B. lokale Benutzer. Ein Unternehmen hat möglicherweise nur eine oder wenige Arbeitsgruppen, so dass sich der Aufbau eines ADs nicht lohnt.

Dieses Unternehmen möchte SafeGuard Enterprise einsetzen, um dann seine Benutzer-/Computerobjekte mit Richtlinien zu versehen. Deshalb wird die Organisationsstruktur des Unternehmens im SafeGuard Management Center folgendermaßen manuell aufgebaut:



Die Objekte bleiben im Verzeichnis .Automatisch registriert. Sie können mit dem SafeGuard Management Center durch Anwendung von Richtlinien auf das Verzeichnis ".Automatisch registriert" verwaltet werden.

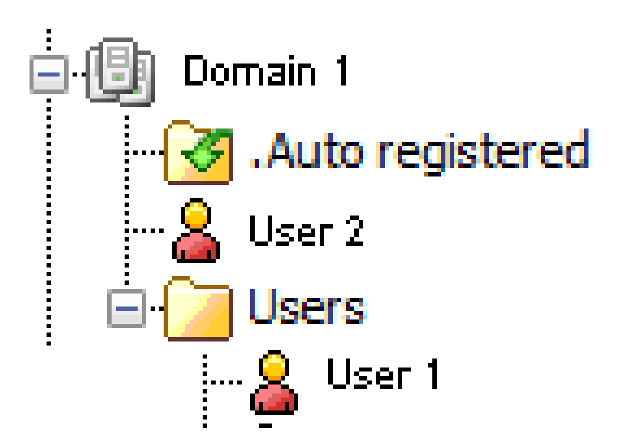
SafeGuard Enterprise Datenbank und Active Directory nicht synchronisiert

Ein Benutzer ist bereits Teil des Active Directory (AD) des Unternehmens. Die SafeGuard Enterprise Datenbank und das AD sind jedoch nicht synchron. Der Benutzer (**Benutzer 1**) meldet sich an SafeGuard Enterprise an und wird automatisch im Bereich **Benutzer und Computer** im SafeGuard Management Center unter der Domäne angezeigt, die durch die Anmeldung vorgegeben ist (**Domäne 1**).



Der Benutzer ist nun Teil des ".Auto regstriert"-Verzeichnisses. Das Objekt kann mit dem SafeGuard Management Center durch Anwendung von Richtlinien auf das ".Automatisch registriert"-Verzeichnis verwaltet werden.

Mit der nächsten Synchronisierung zwischen dem AD und der SafeGuard Enterprise Datenbank wird **Benutzer 1** automatisch in seine Organisationseinheit (**Benutzer**) verschoben..



Damit für **Benutzer 1** jetzt Richtlinien aktiv werden können, müssen sie ab jetzt der Organisationseinheit **Benutzer** zugewiesen werden.

10.2.3 Schlüssel und Zertifikate für autoregistrierte Objekte

Für jedes auto-registrierte Objekt erzeugt der Server nach Bedarf ein Zertifikat.

Ein lokaler Benutzer erhält zwei Schlüssel:

- den Schlüssel des Containers .Automatisch registriert
- den privaten Schlüssel, der vom Server bei Bedarf erzeugt wird.

Lokale Benutzer erhalten keine weiteren Schlüssel der ihnen übergeordneten Container, auch keinen Root-Schlüssel.

Arbeitsgruppen erhalten gar keine Schlüssel.

10.2.4 Richtlinien für autoregistrierte Objekte

Für autoregistrierte Objekte können ohne Einschränkung Richtlinien erstellt werden.

Lokale Benutzer werden zur Gruppe „.authentisierte Benutzer“ hinzugefügt. Computer werden zur Gruppe „.authentisierte Computer“ hinzugefügt. Dementsprechend gelten für sie die Richtlinien, die für diese Gruppe aktiviert wurden.

10.2.5 Erzeugen von Arbeitsgruppen

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie unter dem Stammverzeichnis einen Container erzeugen, der eine Windows Arbeitsgruppe repräsentiert. Arbeitsgruppen erhalten keine Schlüssel. Sie können nicht umbenannt werden.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf **Stamm [Filter ist aktiv]** und wählen Sie im Kontextmenü **Neu > Neue Arbeitsgruppe erzeugen (autom. Registrierung)**.

3. Gehen Sie in **Allgemeine Informationen** wie folgt vor:
   a) Geben Sie einen **vollständigen Namen** für die Arbeitsgruppe ein.
   b) Sie können optional eine **Beschreibung** hinzufügen.
   c) Im Feld **Verbindungsstatus** wird der Typ des Objekts angezeigt, in diesem Fall **Arbeitsgruppe**.
   d) Aktivieren Sie **Richtlinienvererbung stoppen**, wenn gewünscht.
   e) Klicken Sie auf **OK**.

Die Arbeitsgruppe wird erzeugt. Unterhalb des Arbeitsgruppen-Containers wird automatisch das Standardverzeichnis **.Automatisch registriert** angelegt. Es kann weder umbenannt noch gelöscht werden.

10.2.6 Löschen von Arbeitsgruppen

Um eine Arbeitsgruppe zu löschen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für die relevante Arbeitsgruppe. Falls die Arbeitsgruppe Mitglieder hatte, werden diese ebenfalls gelöscht. (Bei der nächsten Anmeldung werden sie wieder autoregistriert).

Um eine Arbeitsgruppe zu löschen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für alle beteiligten Objekte.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Rechts-klicken Sie im rechten Navigationsbereich auf der Arbeitsgruppe, die gelöscht werden soll, und wählen Sie **Löschen**.
3. Klicken Sie zur Bestätigung auf **OK**.

Die Arbeitsgruppe wird gelöscht. Eventuelle Mitglieder werden ebenfalls gelöscht.

Hinweis: Wenn Sie das Zugriffsrecht **Voller Zugriff** nicht für alle Mitglieder der Arbeitsgruppe haben, schlägt das Löschen der Arbeitsgruppe fehl und es wird eine Fehlermeldung angezeigt.

10.2.7 Erstellen einer neuen Domäne

Als Sicherheitsbeauftragter mit den nötigen Berechtigungen können Sie unter dem Stammverzeichnis eine neue Domäne anlegen. Sie sollten nur neue Domänen anlegen, wenn Sie keine Domänen aus dem Active Directory (AD) importieren wollen oder können, z. B. weil kein AD vorhanden ist.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf **Stamm [Filter ist aktiv]** und wählen Sie im Kontextmenü **Neu > Neue Domäne erzeugen (autom. Registrierung)**.
3. In **Allgemeine Informationen** machen Sie folgende Angaben zum Domänen-Controller.

Alle zwei Namenseinträge müssen korrekt sein. Ansonsten wird die Domäne nicht synchronisiert.

a) **Vollst. Name:** z. B. *rechnername.domäne.com* oder die IP-Adresse des Domänen-Controllers

b) **Distinguished Name** (schreibgeschützt): DNS-Name, z. B. **`DC=rechnername3,DC=domäne,DC=Land`**

c) Eine Domänenbeschreibung (optional)

d) **Netbios Name**: Name des Domänen-Controllers

e) Unter **Verbindungsstatus** wird der Typ des Objekts angezeigt, in diesem Fall **Domäne**.

f) Aktivieren Sie **Richtlinienvererbung stoppen**, wenn gewünscht.

g) Klicken Sie auf **OK**.

Die neue Domäne wird angelegt. Ein Benutzer und/oder ein Computer wird bei der Autoregistrierung automatisch dieser Domäne zugeordnet. Unterhalb des Domänen-Containers wird das Standardverzeichnis **.Automatisch registriert** angelegt. Es kann weder umbenannt noch gelöscht werden.

10.2.8 Umbenennen einer Domäne

Als Sicherheitsbeauftragter mit den nötigen Berechtigungen können Sie eine Domäne umbenennen und weitere Eigenschaften für sie festlegen. Sie benötigen das Zugriffsrecht **Voller Zugriff** für die relevante Domäne.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf der Domäne, die umbenannt werden soll, und wählen Sie **Eigenschaften**.
3. Ändern Sie in **Allgemeine Informationen** unter **Vollst. Name** den Namen der Domäne und die Beschreibung.
4. In **Netbios Name** können Sie den Namen des Domänen-Controllers ändern.
5. Außerdem können Sie in der Registerkarte **Containereinstellungen** den Wake-on-LAN-Modus für den automatischen Neustart festlegen.
6. Klicken Sie zur Bestätigung Ihrer Einstellungen auf **OK**.

Die Änderungen sind nun gespeichert.

10.2.9 Löschen einer Domäne

Als Sicherheitsbeauftragter mit den nötigen Berechtigungen können Sie Domänen löschen. Um eine Domäne zu löschen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für die relevante Domäne.

Hinweis: Falls die Domäne Mitglieder hatte, werden diese ebenfalls gelöscht.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Rechts-klicken Sie im linken Navigationsfenster auf der Domäne, die gelöscht werden soll, und wählen Sie **Löschen**.
3. Klicken Sie auf **Ja**.

Die Domäne wird gelöscht. Eventuelle Mitglieder werden ebenfalls gelöscht.

Hinweis: Wenn Sie das Zugriffsrecht **Voller Zugriff** nicht für alle Mitglieder der Domäne haben, schlägt das Löschen der Domäne fehl und es wird eine Fehlermeldung angezeigt.

10.2.10 Löschen von automatisch registrierten Computern

Wenn ein automatisch registrierter Computer gelöscht wird, werden alle lokalen Benutzer dieses Computers ebenfalls gelöscht. Bei der nächsten Anmeldung dieses Computers wird er erneut automatisch registriert.

10.2.11 Filter für lokale Objekte

10.2.11.1 Benutzer und Computer

Unter **Benutzer & Computer** können Sie die Ansicht im linken Navigationsfenster nach lokalen Benutzern filtern oder einen bestimmten lokalen Benutzer suchen.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie links unten im Navigationsbereich auf **Filter**.
3. Wählen Sie bei **Typ** die Option **Lokaler Benutzer**. Wenn Sie einen bestimmten Benutzer suchen, geben Sie noch dessen Namen ein.
4. Klicken Sie auf das Lupen-Symbol.

Die Ansicht auf **Benutzer & Computer** wird entsprechend den Kriterien gefiltert.

Hinweis: Microsoft Konten werden immer als SafeGuard Enterprise Gastbenutzer behandelt.

10.2.11.2 Protokollierung

Die erfolgreiche bzw. nicht erfolgreiche Registrierung eines Benutzers, Computers oder einer Arbeitsgruppe wird protokolliert. Sie können sich diese Informationen im SafeGuard Management Center unter **Berichte** in der Ereignisanzeige auflisten lassen.

10.3 Suche nach Benutzern, Computern und Gruppen in der SafeGuard Enterprise Datenbank

Um Objekte im Dialog **Benutzer, Computer und Gruppen suchen** anzeigen zu lassen, benötigen Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** für die relevanten Objekte.

Hinweis: Wenn Sie nach Objekten suchen, dann bekommen Sie nur Suchergebnisse innerhalb der Bereiche (Domäne), für die Sie Zugriff als Sicherheitsbeauftragter haben. Nur ein Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO) kann einen erfolgreichen Root Search-Prozess durchführen.

Im Bereich **Benutzer & Computer** können Sie mit verschiedenen Filtern nach Objekten suchen. So können Sie z. B. mit dem Filter **Doppelte Benutzer und Computer** nach Duplikaten suchen, die durch einen AD-Synchronisierungsvorgang entstehen können. Der Filter zeigt alle Computer mit demselben Namen in einer Domäne sowie alle Benutzer mit demselben Namen, Anmeldenamen oder Prä-2000 Anmeldenamen in einer Domäne.

So suchen Sie nach Objekten:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsbereich den gewünschten Container.

3. Wählen Sie **Bearbeiten > Suchen** in der SafeGuard Management Center Menüleiste.

   Der **Benutzer, Computer und Gruppen suchen** Dialog wird angezeigt.

4. Wählen Sie den gewünschten Filter aus der **Suchen** Dropdownliste aus.
5. Im Feld **In** wird der ausgewählte Container angezeigt.

   Den hier angezeigten Container können Sie ändern, indem Sie eine andere Option aus der Dropdownliste auswählen.

6. Wenn Sie nach einem bestimmten Objekt suchen, geben Sie den erforderlichen Suchnamen im Feld **Suchname** ein.
7. Legen Sie mit dem Kontrollkästchen **Ansicht nach jeder Suche löschen** fest, ob die Suchergebnisse nach jedem Suchvorgang aus der Ansicht gelöscht werden sollen.
8. Klicken Sie anschließend auf **Jetzt suchen**.

Die Ergebnisse werden im **Benutzer, Computer und Gruppen suchen** Dialog angezeigt. Wenn Sie auf eines der Ergebnisse in diesem Dialog klicken, wird der entsprechende Eintrag in der **Benutzer & Computer** Baumstruktur markiert. Wenn Sie z. B. nach Duplikaten gesucht haben, können Sie diese nun bequem löschen.

10.4 Anzeigen von Objekteigenschaften in Benutzer und Computer

Um Objekteigenschaften einzusehen, benötigten Sie die Zugriffsrechte **Voller Zugriff** oder **Schreibgeschützt** für die relevanten Objekte.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie im Navigationsbereich von **Benutzer & Computer** mit der rechten Maustaste auf das gewünschte Objekt und wählen Sie **Eigenschaften**.

Die Eigenschaften des ausgewählten Objekts werden angezeigt. Wenn Sie für das Objekt das Zugriffsrecht **Schreibgeschützt** haben, werden die Eigenschaften im Dialog ausgegraut und Sie können diese nicht bearbeiten.

11 SafeGuard Enterprise Sicherheitsbeauftragte

SafeGuard Enterprise kann von einem oder mehreren Sicherheitsbeauftragten administriert werden. Mit der rollenbasierten Administration ist es möglich, die Verwaltung von SafeGuard Enterprise auf mehrere Benutzer zu verteilen. Dabei kann einem Benutzer eine oder mehrere Rollen zugewiesen werden. Um die Sicherheit noch zu erhöhen, kann einer Sicherheitsbeauftragtenrolle die zusätzliche Autorisierung eines Vorgangs zugewiesen werden.

Während der initialen Konfiguration des SafeGuard Management Center wird automatisch ein Administrator höchster Ebene angelegt: der Haupt-Sicherheitsbeauftragte (Master Security Officer, MSO). Das MSO Zertifikat wird standardmäßig nach 5 Jahren ungültig und kann im Management Center im Abschnitt **Sicherheitsbeauftragte** erneuert werden. Für andere spezifische Aufgaben, z. B. Helpdesk- oder Audit-Aufgaben, können dann weitere Sicherheitsbeauftragte zugewiesen werden.

Sicherheitsbeauftragte lassen sich im Navigationsbereich des SafeGuard Management Center gemäß der Organisationsstruktur Ihres Unternehmens hierarchisch anordnen. Diese hierarchische Anordnung gibt jedoch keine Hierarchie in Bezug auf Rechte und Rollen wieder.

Hinweis: Zwei Sicherheitsbeauftragte dürfen nicht das gleiche Windows-Konto auf einem Computer benutzen. Andernfalls lassen sich ihre Zugriffsrechte nicht sauber trennen. Unter Umständen ist die zusätzliche Autorisierung nur dann sinnvoll, wenn sich die Sicherheitsbeauftragten mit kryptographischen Token/Smartcards anmelden müssen.

11.1 Rollen für Sicherheitsbeauftragte

SafeGuard Enterprise bietet für die komfortable Verwaltung bereits vordefinierte Rollen mit verschiedenen Funktionen für Sicherheitsbeauftragte an. Ein Sicherheitsbeauftragter mit den erforderlichen Rechten hat die Möglichkeit, aus einer Liste von Aktionen/Rechten selbst neue Rollen zu definieren und bestimmten Sicherheitsbeauftragten zuzuweisen.

Folgende Rollentypen stehen zur Verfügung:

- Rolle des Haupt-Sicherheitsbeauftragten (Master Security Officer, MSO)
- Vordefinierte Rollen
- Benutzerdefinierte Rollen

11.1.1 Haupt-Sicherheitsbeauftragter

Nach der Installation von SafeGuard Enterprise wird bei der initialen Konfiguration des SafeGuard Management Center automatisch ein Haupt-Sicherheitsbeauftragter (Master Security Officer, MSO) angelegt. Der Haupt-Sicherheitsbeauftragte ist der Sicherheitsbeauftragte der höchsten Ebene und hat alle Rechte sowie Zugriff auf alle Objekte, vergleichbar mit dem Administrator bei Windows. Die Rechte des Haupt-Sicherheitsbeauftragten können nicht geändert werden.

Für eine Instanz des SafeGuard Management Centers können mehrere Haupt-Sicherheitsbeauftragte angelegt werden. Aus Sicherheitsgründen empfehlen wir,

mindestens einen weiteren Haupt-Sicherheitsbeauftragten anzulegen. Zusätzliche Haupt-Sicherheitsbeauftragte können jederzeit gelöscht werden, es muss jedoch immer ein Benutzer mit der Rolle des Haupt-Sicherheitsbeauftragten vorhanden sein, der explizit als Hauptsicherheits-Beauftragter in der SafeGuard Enterprise Datenbank angelegt wurde.

Ein Haupt-Sicherheitsbeauftragter kann Aufgaben an andere Personen delegieren. Dazu gibt es zwei Möglichkeiten:

- Ein neuer Benutzer/Sicherheitsbeauftragter kann unter **Sicherheitsbeauftragte** angelegt werden.
- Ein aus dem Active Directory importierter und im Stammverzeichnis des SafeGuard Management Center sichtbarer Benutzer oder alle Mitglieder eines Containers können unter **Benutzer & Computer** zu Sicherheitsbeauftragten gemacht werden.

Den Sicherheitsbeauftragten können eine oder mehrere Rollen zugeordnet werden. Einem Benutzer kann z. B. die Rolle des Verwaltungsbeauftragten und die Rolle des Helpdesk-Beauftragten zugewiesen werden.

Der Haupt-Sicherheitsbeauftragte kann aber auch selbst definierte Rollen anlegen und bestimmten Sicherheitsbeauftragten zuweisen.

11.1.2 Vordefinierte Rollen

Im SafeGuard Management Center sind neben dem Haupt-Sicherheitsbeauftragten die folgenden Rollen vordefiniert. Die diesen vordefinierten Rollen zugewiesenen Rechte können nicht geändert werden. Verfügt eine vordefinierte Rolle z. B. über das Recht „Richtlinien und Richtliniengruppen erstellen“, so kann dieses Recht nicht aus der Rolle entfernt werden. Es können auch keine neuen Rechte zu einer vordefinierten Rollen hinzugefügt werden. Die zusätzliche Autorisierung durch einen weiteren Sicherheitsbeauftragten hingegen lässt sich jederzeit den vordefinierten Rollen zuordnen.

- **Verwaltungsbeauftragter**

  Verwaltungsbeauftragte können Ihren eigenen Knoten im Bereich **Sicherheitsbeauftragte** einsehen und sind dazu berechtigt, die ihrem Knoten zugehörigen Sicherheitsbeauftragten zu verwalten.

- **Sicherheitsbeauftragter**

  Sicherheitsbeauftragte haben umfassende Rechte u. a. für die SafeGuard Enterprise Konfiguration, Richtlinien- und Schlüsselverwaltung sowie für Überwachung und Recovery.

- **Helpdesk-Beauftragter**

  Helpdesk-Beauftragte sind zur Durchführung von Recovery-Vorgängen berechtigt. Darüber hinaus können sie sich die meisten Funktionsbereiche des SafeGuard Management Center anzeigen lassen.

- **Audit-Beauftragter**

  Um SafeGuard Enterprise überwachen zu können, haben Audit-Beauftragte die Berechtigung, sich die meisten Funktionsbereiche des SafeGuard Management Center anzeigen zu lassen.

- **Recovery-Beauftragter**

  Recovery-Beauftragte sind dazu berechtigt, die SafeGuard Enterprise Datenbank zu reparieren.

11.1.3 Benutzerdefinierte Rollen

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie neue Rollen aus einer Liste mit Aktionen/Rechten definieren und sie einem vorhandenen oder einem neuen Sicherheitsbeauftragten zuweisen. Wie auch bei den vordefinierten Rollen lässt sich die zusätzliche Autorisierung durch einen weiteren Sicherheitsbeauftragten für eine Funktion der betreffenden Rolle jederzeit aktivieren.

Bei der Zuweisung einer neuen Rolle ist für die zusätzliche Autorisierung Folgendes zu beachten:

Hinweis: Wenn ein Benutzer zwei Rollen mit der gleichen Funktion inne hat, und bei einer der Rollen die zusätzliche Autorisierung zugeordnet ist, dann gilt das automatisch auch bei der anderen Rolle.

Ein Sicherheitsbeauftragter mit den erforderlichen Rechten kann Rechte zu einer benutzerdefinierten Rolle hinzufügen oder Rechte aus der Rolle entfernen. Im Gegensatz zu vordefinierten Rollen können benutzerdefinierte je nach Anforderung auch gelöscht werden. Wird die Rolle gelöscht, so ist sie keinem Benutzer mehr zugewiesen. Ist einem Benutzer nur eine Rolle zugewiesen und wird diese Rolle gelöscht, so kann sich der Benutzer nicht mehr am SafeGuard Management Center anmelden.

Hinweis: Die Rolle und die darin definierten Aktionen bestimmen, was ein Benutzer darf und was nicht. Auch dann, wenn dem Benutzer mehrere Rollen zugewiesen worden sind. Nachdem er sich am System angemeldet hat, werden nur die Bereiche des SafeGuard Management Centers aktiviert und angezeigt, die für seine Rolle nötig sind. Das betrifft auch die Bereiche Skripte und API. Sie sollten deshalb immer die Anzeige des Bereichs aktivieren, in dem die betreffenden Aktionen definiert sind. Aktionen werden nach Funktionsbereich sortiert und sind hierarchisch strukturiert. Diese Struktur zeigt, welche Aktionen vor der Durchführung bestimmter anderer Aktionen erforderlich sind.

11.1.4 Zusätzliche Autorisierung

Die zusätzliche Autorisierung (auch Vier-Augen-Prinzip genannt) kann spezifischen Aktionen einer Rolle zugeordnet werden. Das bedeutet, dass der Benutzer dieser Rolle eine bestimmte Aktion nur ausführen darf, wenn ein Benutzer einer weiteren Rolle anwesend ist und die Ausführung der Aktion bestätigt. Jedes Mal, wenn ein Benutzer diese Aktion ausführt, muss ein anderer Benutzer sie bestätigen.

Die zusätzliche Autorisierung lässt sich sowohl vordefinierten als auch benutzerdefinierten Rollen zuweisen. Sobald es zumindest noch einen Beauftragten mit der gleichen Rolle gibt, kann auch die eigene Rolle ausgewählt werden.

Die Rolle, die die zusätzliche Autorisierung durchführen soll, muss einem Benutzer zugewiesen sein und es müssen mindestens zwei Benutzer in der SafeGuard Datenbank vorhanden sein. Wenn die zusätzliche Autorisierung für eine Aktion erforderlich ist, ist sie auch dann erforderlich, wenn der Benutzer eine weitere Rolle hat, die die zusätzliche Autorisierung für diese Aktion nicht erfordert.

Wenn ein Sicherheitsbeauftragter ohne Berechtigung zum Ändern der Einstellungen für die zusätzliche Autorisierung eine Rolle anlegt, werden die Einstellungen für die zusätzliche Autorisierung der neuen Rolle gemäß den definierten Einstellungen für den anlegenden Benutzer voreingestellt.

11.2 Anlegen einer neuen Rolle

Voraussetzung: Um eine neue Rolle anzulegen, benötigen Sie das Recht, benutzerdefinierte Rollen einzusehen und zu verwalten. Um die zusätzliche Autorisierung zuzuweisen, benötigen Sie das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie mit der rechten Maustaste auf **Benutzerdefinierte Rollen** und wählen Sie **Neu > Neue benutzerdefinierte Rolle**.
3. Geben Sie im Dialog **Neue benutzerdefinierte Rolle** einen Namen und eine Beschreibung für die Rolle ein.
4. Wählen Sie die Aktionen für diese Rolle: Wählen Sie die Kontrollkästchen neben den gewünschten Aktionen in der Spalte **Aktiv**.

   Aktionen werden nach Funktionsbereich sortiert und sind hierarchisch strukturiert. Diese Struktur zeigt, welche Aktionen vor der Durchführung bestimmter anderer Aktionen erforderlich sind.

5. Falls erforderlich, weisen Sie die **zusätzliche Autorisierung** zu: Klicken Sie auf die Standardeinstellung **Kein** und wählen Sie die gewünschte Rolle aus der angezeigten Dropdownliste.

   Wenn ein Sicherheitsbeauftragter ohne die Berechtigung zum Ändern der zusätzlichen Autorisierung eine Rolle anlegt, wird die zusätzliche Autorisierung gemäß den Einstellungen der Rolle des betreffenden Sicherheitsbeauftragten vordefiniert.

6. Klicken Sie auf **OK**.

Die neue Rolle wird unter **Benutzerdefinierte Rollen** im Navigationsfenster angezeigt. Wenn Sie die Rolle anklicken, werden im rechten Aktionsbereich die zulässigen Aktionen dargestellt.

11.3 Zuweisen einer Rolle zu einem Sicherheitsbeauftragten

Voraussetzung: Um eine Rolle zuzuweisen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu ändern.

1. Wählen Sie den gewünschten Sicherheitsbeauftragten im Navigationsfenster aus.

   Die Eigenschaften werden im rechten Aktionsbereich für ihn angezeigt.

2. Weisen Sie die gewünschten Rollen durch Auswählen der entsprechenden Kontrollkästchen zu.

   Vordefinierte Rollen werden fett angezeigt.

3. Klicken Sie auf das Doppelpfeil-Symbol **Aktualisieren** in der Symbolleiste.

Die Rolle ist dem Sicherheitsbeauftragten zugewiesen.

Hinweis: Komplexe, individuell angepasste Rollen können leichte Performanceprobleme bei der Benutzung des SafeGuard Management Centers verursachen.

11.4 Einsehen von Sicherheitsbeauftragten- und Rolleneigenschaften

Voraussetzung: Um sich einen Überblick über die Sicherheitsbeauftragteneigenschaften oder die Rollenzuordnungen anzeigen zu lassen, benötigen Sie das Recht zum Einsehen von Sicherheitsbeauftragten und Sicherheitsbeauftragtenrollen.

So sehen Sie Sicherheitsbeauftragten- und Rolleneigenschaften ein:

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Doppelklicken Sie im Navigationsbereich auf der linken Seite auf dem Objekt, zu dem Sie einen Überblick erhalten möchten.

Die im Aktionsbereich angezeigten Informationen richten sich nach dem ausgewählten Objekt.

11.4.1 Anzeigen der Eigenschaften für den Haupt-Sicherheitsbeauftragten

Die allgemeinen Informationen sowie die Änderungsinformationen für den Haupt-Sicherheitsbeauftragten werden angezeigt.

11.4.2 Anzeigen der Eigenschaften für Sicherheitsbeauftragte

Die allgemeinen Informationen sowie die Änderungsinformationen für den Sicherheitsbeauftragten werden angezeigt.

1. Wählen Sie unter **Eigenschaften** die Registerkarte **Aktionen**. Diese Registerkarte bietet eine Zusammenfassung der zulässigen Aktionen sowie der Rollen, die dem Sicherheitsbeauftragten zugewiesen sind.

11.4.3 Anzeigen der Rechte und Rollen von Sicherheitsbeauftragten

Eine Zusammenfassung der Aktionen aller Rollen, die dem Sicherheitsbeauftragten zugewiesen sind, wird angezeigt. Die Baumstrukturansicht zeigt, welche Aktionen erforderlich sind, damit bestimmte andere Aktionen durchgeführt werden können. Darüber hinaus können die zugewiesenen Rollen angezeigt werden.

1. Wählen Sie in den **<Sicherheitsbeauftragtenname> Eigenschaften** in der Registerkarte **Aktionen** eine Aktion, um alle zugewiesenen Rollen aufzurufen, die diese Aktion enthalten.
2. Doppelklicken Sie in der Liste **Zugewiesene Rollen mit ausgewählter Aktion** auf einer Rolle. Der **<Sicherheitsbeauftragtenname> Eigenschaften** Dialog wird geschlossen und die Eigenschaften der Rolle werden angezeigt.

11.4.4 Anzeigen der Rolleneigenschaften

Die allgemeinen Informationen sowie die Änderungsinformationen für die Rolle werden angezeigt.

1. Wählen Sie unter **Eigenschaften** die Registerkarte **Zuweisung**, um die Sicherheitsbeauftragten anzeigen zu lassen, die dieser Rolle zugeordnet sind.

11.4.5 Anzeigen der Rollenzuordnung

1. Doppelklicken Sie in den **<Rollenname> Eigenschaften** in der Registerkarte **Zuweisung** auf einem Sicherheitsbeauftragten. Der **Eigenschaften** Dialog wird geschlossen und es werden die allgemeinen Daten und die Rollen des Sicherheitsbeauftragten angezeigt.

11.5 Ändern einer Rolle

Für das Ändern von Rollen gibt es folgende Möglichkeiten:

- Zusätzliche Autorisierung ändern
- Sie können alle Eigenschaften der Rolle ändern.

Das Symbol neben den Rollen zeigt, welche Aktion möglich ist:

Symbol	Beschreibung
	Die Rolle kann geändert werden (Aktionen hinzufügen/löschen).
	Die zusätzliche Autorisierung kann geändert werden.
	Beide Änderungsmöglichkeiten sind verfügbar.

Hinweis: Vordefinierte Rollen und die ihnen zugewiesenen Aktionen können nicht geändert werden. Ist die zusätzliche Autorisierung aktiviert, so kann dies für jede Rolle, auch für vordefinierte Rollen, geändert werden.

11.5.1 Ändern der zusätzlichen Autorisierung

Voraussetzung: Um die zusätzliche Autorisierung zuzuweisen, benötigen Sie das Recht, Sicherheitsbeauftragtenrollen einzusehen sowie das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** auf die Rolle, die Sie ändern möchten. Klicken Sie im Aktionsbereich auf der rechten Seite bei der gewünschten Einstellung in der Spalte **Zusätzliche Autorisierung** und wählen Sie eine andere Rolle aus der Liste aus.

   Vordefinierte Rollen werden fett angezeigt.

3. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die zusätzliche Autorisierung für diese Rolle wurde geändert.

11.5.2 Ändern aller Eigenschaften einer Rolle

Voraussetzung: Um eine benutzerdefinierte Rolle zu ändern, benötigen Sie das Recht zum Einsehen und Ändern von Sicherheitsbeauftragtenrollen. Zum Ändern der Einstellung für die zusätzliche Autorisierung benötigen Sie außerdem das Recht „Einstellungen für zusätzliche Autorisierung ändern“.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** auf die Rolle, die Sie ändern möchten, und wählen Sie **Benutzerdefinierte Rolle ändern**.
3. Ändern Sie die Eigenschaften nach Wunsch. Ändern Sie die Einstellungen für die zusätzliche Autorisierung, indem Sie auf den Wert in dieser Spalte klicken und die gewünschte Rolle auswählen.
4. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die Rolle wurde geändert.

11.6 Kopieren einer Rolle

Um eine Rolle anzulegen, die ähnliche Eigenschaften wie eine bereits vorhandene Rolle hat, können Sie die vorhandene Rolle als Vorlage benutzen. Sie können eine vordefinierte oder eine benutzerdefinierte Rolle als Vorlage auswählen.

Voraussetzung: Die Verwendung von vorhandenen Rollen als Vorlage ist nur dann möglich, wenn der derzeit authentisierte Sicherheitsbeauftragte alle Rechte hat, die in dieser spezifischen Rollenvorlage enthalten sind. Diese Funktion ist also u. U. für Sicherheitsbeauftragte, deren zulässige Aktionen begrenzt sind, nicht verfügbar.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf die Rolle, die Sie kopieren möchten, und wählen Sie **Neu > Neue Kopie der Rolle**. Unter **Neue benutzerdefinierte Rolle** werden alle Eigenschaften der vorhandenen Rolle bereits vorausgewählt.
3. Geben Sie einen neuen Namen für diese Rolle ein und ändern Sie die Eigenschaften nach Wunsch.
4. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die neue Rolle ist angelegt.

11.7 Löschen einer Rolle

Hinweis: Vordefinierte Rollen können nicht gelöscht werden.

Voraussetzung: Um eine Rolle zu löschen, benötigen Sie das Recht zum Einsehen und Löschen von Sicherheitsbeauftragtenrollen.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.

2. Klicken Sie im Navigationsfenster unter **Benutzerdefinierte Rollen** mit der rechten Maustaste auf die Rolle, die Sie löschen möchten, und wählen Sie **Löschen**. Je nach den Eigenschaften der Rolle wird eine entsprechende Warnungsmeldung angezeigt.

   Hinweis: Wenn Sie eine Rolle löschen, geht diese Rolle bei allen Sicherheitsbeauftragten, denen sie zugeordnet ist, verloren. Ist einem Sicherheitsbeauftragten nur diese eine Rolle zugewiesen, so kann dieser sich erst wieder am SafeGuard Management Center anmelden, wenn ein übergeordneter Sicherheitsbeauftragter ihm eine neue Rolle zuweist. Wird die Rolle für die zusätzliche Autorisierung verwendet, so wird der Haupt-Sicherheitsbeauftragte dazu aufgefordert, die zusätzliche Autorisierung durchzuführen.

3. Um die Rolle zu löschen, klicken Sie in der Warnungsmeldung auf **Ja**.
4. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die Rolle wird aus dem Navigationsfenster entfernt und aus der Datenbank gelöscht.

11.8 Anlegen eines Haupt-Sicherheitsbeauftragten

Voraussetzung: Um einen neuen Haupt-Sicherheitsbeauftragten anzulegen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und anzulegen.

Hinweis: Ein schneller Weg, einen neuen Haupt-Sicherheitsbeauftragten zu erstellen, ist, einen Sicherheitsbeauftragter höher zu stufen. Weitere Informationen finden Sie unter Höherstufen von Sicherheitsbeauftragten (Seite 66).

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Knoten **Haupt-Sicherheitsbeauftragte** und wählen Sie **Neu > Neuer Haupt-Sicherheitsbeauftragter**.

3. Nehmen Sie die relevanten Einträge unter Neuer Haupt-**Sicherheitsbeauftragter** vor:

Feld/Kontrollkästchen	Beschreibung
Freigeschaltet	Hier kann der Sicherheitsbeauftragte bis auf Weiteres deaktiviert werden. Das bedeutet, dass er zwar im System existiert, sich aber noch nicht an das SafeGuard Management Center anmelden kann. Erst wenn er durch einen anderen Sicherheitsbeauftragten aktiviert wird, kann er sich anmelden und seine administrativen Tätigkeiten ausführen.
Name	Hier wird der Name des Sicherheitsbeauftragten angegeben, wie er in den von SafeGuard Enterprise erzeugten Zertifikaten unter cn= eingetragen wird. Unter diesem Namen wird er auch im Navigationsfenster des SafeGuard Management Centers angezeigt. Dieser Name muss eindeutig sein. Maximalwert: 256 Zeichen
Beschreibung	Optional Maximalwert: 256 Zeichen
Mobiltelefon	Optional Maximalwert: 128 Zeichen
E-Mail	Optional Maximalwert: 256 Zeichen
Token-Anmeldung	Die Anmeldung kann auf folgende Art erfolgen: **Ohne Token** Der Sicherheitsbeauftragte darf sich nicht mit einem Token anmelden. Er muss sich über die Anmeldeinformationen (Benutzername/Kennwort) anmelden. **Optional** Die Anmeldung kann mit Token oder mit Anmeldeinformationen erfolgen. Der Sicherheitsbeauftragte kann wählen. **Zwingend erforderlich** Die Verwendung eines Token zur Anmeldung ist zwingend vorgeschrieben. Dazu muss sich der zum Zertifikat des Sicherheitsbeauftragten gehörende private Schlüssel auf dem Token befinden.

Feld/Kontrollkästchen	Beschreibung
Zertifikat	Zur Anmeldung an das SafeGuard Management Center benötigt ein Sicherheitsbeauftragter immer ein Zertifikat. Das Zertifikat kann entweder von SafeGuard Enterprise selbst erstellt werden oder es wird ein bereits existierendes verwendet. Ist eine Anmeldung mit Token zwingend notwendig, so muss das Zertifikat auf den Token des Sicherheitsbeauftragten aufgebracht werden. **Erzeugen:** Zertifikat und Schlüsseldatei werden erstellt und an einem auswählbaren Ort gespeichert. Dabei muss ein Kennwort für die .p12-Schlüsseldatei angegeben und bestätigt werden. Die .p12-Datei muss dem Sicherheitsbeauftragten bei der Anmeldung zur Verfügung stehen. Das erstellte Zertifikat wird dem Sicherheitsbeauftragten automatisch zugeteilt und unter **Zertifikat** angezeigt. Wenn SafeGuard Enterprise Kennwortregeln angewendet werden, sollten die Regeln im Active Directory deaktiviert werden. **Hinweis:** Maximale Länge des Speicherpfads und des Dateinamens: 260 Zeichen. Zum Anlegen eines Sicherheitsbeauftragten ist der öffentliche Teil des Zertifikats zwar ausreichend. Bei der Anmeldung an das SafeGuard Management Center ist jedoch auch der private Teil des Zertifikats (die Schlüsseldatei) erforderlich. Liegt diese nicht in der Datenbank vor, muss sie dem Sicherheitsbeauftragten zur Verfügung stehen und kann bei der Anmeldung dann ggf. im Zertifikatsspeicher abgelegt werden.
Zertifikat	**Importieren:** Ein existierendes Zertifikat wird importiert und anschließend dem Sicherheitsbeauftragten zugewiesen. Wird aus einer .p12 Schlüsseldatei importiert, muss das Kennwort des Zertifikats bekannt sein. Wird ein PKCS#12 Zertifikatscontainer ausgewählt, werden alle Zertifikate in die Liste der zuweisbaren Zertifikate geladen. Die Zuweisung des Zertifikats erfolgt nach dem Import, indem das Zertifikat im Dropdown-Listenfeld ausgewählt wird.

4. Klicken Sie zur Bestätigung Ihrer Einstellungen auf **OK**.

Der neu angelegte Haupt-Sicherheitsbeauftragte wird im Navigationsfenster unter dem Knoten **Haupt-Sicherheitsbeauftragte** angezeigt. Die jeweiligen Eigenschaften lassen sich durch Auswahl des gewünschten Sicherheitsbeauftragten im Navigationsfenster anzeigen. Der Haupt-Sicherheitsbeauftragte kann sich mit dem angezeigten Namen an das SafeGuard Management Center anmelden.

11.9 Anlegen eines Sicherheitsbeauftragten

Voraussetzung: Um einen neuen Sicherheitsbeauftragten anzulegen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und anzulegen.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten-Knoten, in dem Sie den neuen Sicherheitsbeauftragten anlegen möchten, und wählen Sie **Neu > Neuer Sicherheitsbeauftragter**.

3. Nehmen Sie die relevanten Einträge unter **Neuer Sicherheitsbeauftragter** vor:

Feld/Kontrollkästchen	Beschreibung
Freigeschaltet	Hier kann der Sicherheitsbeauftragte bis auf Weiteres deaktiviert werden. Das bedeutet, dass er zwar im System existiert, sich aber noch nicht an das SafeGuard Management Center anmelden kann. Erst wenn er durch einen anderen Sicherheitsbeauftragten aktiviert wird, kann er sich anmelden und seine administrativen Tätigkeiten ausführen.
Name	Hier wird der Name des Sicherheitsbeauftragten angegeben, wie er in den von SafeGuard Enterprise erzeugten Zertifikaten unter cn= eingetragen wird. Unter diesem Namen wird er auch im Navigationsfenster des SafeGuard Management Centers angezeigt. Dieser Name muss eindeutig sein. Maximalwert: 256 Zeichen
Beschreibung	Optional Maximalwert: 256 Zeichen
Mobiltelefon	Optional Maximalwert: 128 Zeichen
E-Mail	Optional Maximalwert: 256 Zeichen
Gültig von/bis	Hier wird angegeben, ab und bis wann (Datum) sich der Sicherheitsbeauftragte am SafeGuard Management Center anmelden darf.
Token-Anmeldung	Die Anmeldung kann auf folgende Art erfolgen: **Ohne Token** Der Sicherheitsbeauftragte darf sich nicht mit einem Token anmelden. Er muss sich über die Anmeldeinformationen (Benutzername/Kennwort) anmelden. **Optional** Die Anmeldung kann mit Token oder mit Anmeldeinformationen erfolgen. Der Sicherheitsbeauftragte kann wählen. **Zwingend erforderlich** Die Verwendung eines Token zur Anmeldung ist zwingend vorgeschrieben. Dazu muss sich der zum Zertifikat des Sicherheitsbeauftragten gehörende private Schlüssel auf dem Token befinden.

Feld/Kontrollkästchen	Beschreibung
Zertifikat	Zur Anmeldung an das SafeGuard Management Center benötigt ein Sicherheitsbeauftragter immer ein Zertifikat. Das Zertifikat kann entweder von SafeGuard Enterprise selbst erstellt werden oder es wird ein bereits existierendes verwendet. Ist eine Anmeldung mit Token zwingend notwendig, so muss das Zertifikat auf den Token des Sicherheitsbeauftragten aufgebracht werden. **Erzeugen:** Zertifikat und Schlüsseldatei werden neu erstellt und an einem auswählbaren Ort gespeichert. Dabei muss ein Kennwort für die .p12-Schlüsseldatei angegeben und bestätigt werden. Die .p12-Datei muss dem Sicherheitsbeauftragten bei der Anmeldung zur Verfügung stehen. Das erstellte Zertifikat wird dem Sicherheitsbeauftragten automatisch zugeteilt und unter **Zertifikat** angezeigt. Wenn SafeGuard Enterprise Kennwortregeln angewendet werden, sollten die Regeln im Active Directory deaktiviert werden. **Hinweis:** Maximale Länge des Speicherpfads und des Dateinamens: 260 Zeichen. Zum Anlegen eines Sicherheitsbeauftragten ist der öffentliche Teil des Zertifikats zwar ausreichend. Bei der Anmeldung an das SafeGuard Management Center ist jedoch auch der private Teil des Zertifikats (die Schlüsseldatei) erforderlich. Liegt diese nicht in der Datenbank vor, muss sie dem Sicherheitsbeauftragten zur Verfügung stehen und kann bei der Anmeldung dann ggf. im Zertifikatsspeicher abgelegt werden.
Zertifikat	**Importieren:** Ein existierendes Zertifikat wird importiert und anschließend dem Sicherheitsbeauftragten zugewiesen. Wird aus einer .p12 Schlüsseldatei importiert, muss das Kennwort des Zertifikats bekannt sein. Wird ein PKCS#12 Zertifikatscontainer ausgewählt, werden alle Zertifikate in die Liste der zuweisbaren Zertifikate geladen. Die Zuweisung des Zertifikats erfolgt nach dem Import, indem das Zertifikat im Dropdown-Listenfeld ausgewählt wird.
Rollen des Sicherheitsbeauftragten	**Rollen** Dem Sicherheitsbeauftragten können vordefinierte oder benutzerdefinierte Rollen zugewiesen werden. Die mit jeder Rolle verbundenen Rechte werden unter **Zugelassene Aktion** im Aktionsbereich angezeigt, wenn Sie auf die entsprechende Rolle klicken oder auf den Sicherheitsbeauftragten rechts-klicken und **Eigenschaften**, **Aktionen** wählen. Einem Benutzer können mehrere Rollen zugewiesen werden. Vordefinierte Rollen werden fett dargestellt.

4. Klicken Sie zur Bestätigung Ihrer Einstellungen auf **OK**.

Der neu angelegte Sicherheitsbeauftragte wird im Navigationsfenster unter dem jeweiligen **Sicherheitsbeauftragten** Knoten angezeigt. Die jeweiligen Eigenschaften lassen sich durch Auswahl des gewünschten Sicherheitsbeauftragten im Navigationsfenster anzeigen. Der Sicherheitsbeauftragte kann sich mit dem angezeigten Namen an das SafeGuard Management

Center anmelden. Im nächsten Schritt müssen Sie nun dem Sicherheitsbeauftragten Verzeichnisobjekte/Domänen zuweisen, damit dieser die erforderlichen Aufgaben ausführen kann.

11.10 Zuweisen von Verzeichnisobjekten zu einem Sicherheitsbeauftragten

Für die Ausführung ihrer Aufgaben benötigen Sicherheitsbeauftragte Zugriffsrechte für Verzeichnisobjekte. Zugriffsrechte können für Domänen, Organisationseinheiten (OUs) und Benutzergruppen sowie für den ".Automatisch registriert" Knoten unter dem Stammverzeichnis erteilt werden.

Unter **Benutzer & Computer** können Sie die Zugriffsrechte eines anderen Sicherheitsbeauftragten ändern, wenn Sie vollen Zugriff auf den relevanten Container haben und für den Sicherheitsbeauftragten verantwortlich sind. Ihre eigenen Zugriffsrechte können Sie nicht ändern. Wenn Sie einen Sicherheitsbeauftragten einem Verzeichnisobjekt zum ersten Mal zuweisen, erbt der Sicherheitsbeauftragte Ihre Zugriffsrechte für diesen Container.

Hinweis: Sie können anderen Sicherheitsbeauftragten nicht höhere Zugriffsrechte als Ihre Zugriffsrechte erteilen.

Voraussetzung: Wenn Sie einem Sicherheitsbeauftragten das Recht, auf Verzeichnisobjekte zuzugreifen und diese zu verwalten, gewähren/verweigern möchten, benötigen Sie die "Benutzer und Computer"-Rechte "Zugriffsrechte von Sicherheitsbeauftragten anzeigen" und "Zugriffsrechte für Verzeichnis erteilen/verweigern". Darüber hinaus benötigen Sie das Zugriffsrecht **Voller Zugriff** für das relevante Verzeichnisobjekt.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsfenster auf der linken Seite die gewünschten Verzeichnisobjekte aus.

   Hinweis: Die Navigationsbaumstruktur zeigt nur die Verzeichnisobjekte, für die Sie Zugriffsrechte haben. Wenn Sie das Zugriffsrecht **Voller Zugriff** haben, wird das jeweilige Objekt schwarz dargestellt. Objekte mit Zugriffsrecht **Schreibgeschützt**, werden blau dargestellt. Auf einen ausgegrauten Knoten können Sie nicht zugreifen. Dieser wird jedoch angezeigt, wenn es untergeordnete Knoten gibt, auf die Sie Zugriff haben.

3. Klicken Sie im Aktionsbereich auf der rechten Seite auf die Registerkarte **Zugriff**.
4. Um die Rechte für die ausgewählten Objekte zuzuweisen, ziehen Sie den gewünschten Sicherheitsbeauftragten von der äußersten rechten Seite per Drag&Drop in die **Zugriff** Tabelle.
5. Wählen Sie in der Spalte **Zugriffsrechte** die Rechte, die Sie dem Sicherheitsbeauftragten für die ausgewählten Objekte erteilen möchten.
   - **Voller Zugriff**
   - **Schreibgeschützt**
   - **Verweigert**

   Um die Zuweisung der Rechte für die ausgewählten Objekte rückgängig zu machen, ziehen Sie den Sicherheitsbeauftragten wieder zurück in die Tabelle **Sicherheitsbeauftragte**.

6. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

Die ausgewählten Objekte stehen dem relevanten Sicherheitsbeauftragten zur Verfügung.

Hinweis: Wenn zwei Sicherheitsbeauftragte gleichzeitig mit der gleichen SafeGuard Enterprise Datenbank arbeiten und einer der beiden ändert Zugriffsrechte, wird eine Meldung angezeigt,

die den anderen Sicherheitsbeauftragten darüber informiert. In diesem Fall gehen alle nicht gespeicherten Änderungen verloren. Verliert ein Sicherheitsbeauftragter alle Zugriffsrechte für einen Knoten, so wird der Zugriff nicht mehr gewährt und es wird eine entsprechende Meldung angezeigt. Das Navigationsfenster wird entsprechend aktualisiert.

11.10.1 Einsehen der Sicherheitsbeauftragtenrechte für Verzeichnisobjekte

Die Sicherheitsbeauftragten zugewiesenen Rechte für Verzeichnisobjekte werden in der Registerkarte **Zugriff** der relevanten Objekte unter **Benutzer & Computer** angezeigt.

Hinweis: Die Registerkarte **Zugriff** zeigt nur die Zugriffsrechte für Container, für die Sie Zugriffsrechte haben. Es werden auch nur die Sicherheitsbeauftragten angezeigt, für die Sie verantwortlich sind.

Die Registerkarte **Zugriff** enthält folgende Informationen:

- Die Spalte **Sicherheitsbeauftragte** zeigt die Typen und Namen der den Verzeichnisobjekten zugeordneten Sicherheitsbeauftragten.
- Die Spalte **Zugewiesen von** zeigt den Sicherheitsbeauftragten, der die Zugriffsrechte zugewiesen hat.
- Das **Zuweisungsdatum**
- Die Spalte **Zugriffsrechte** zeigt die erteilten Rechte: **Voller Zugriff**, **Verweigert** oder **Schreibgeschützt**.
- Die Spalte **Ursprung** zeigt den vollständigen Namen des Knotens, an dem das Zugriffsrecht dem entsprechenden Sicherheitsbeauftragten zugewiesen wurde. Zum Beispiel: Wurde das Recht einem übergeordneten Knoten des ausgewählten Verzeichnisobjekts zugewiesen, so wird hier der übergeordnete Knoten angezeigt. In diesem Fall hat der Sicherheitsbeauftragte das Zugriffsrecht für das ausgewählte Verzeichnisobjekt durch Zuweisung an den übergeordneten Knoten geerbt.
- Die Spalte **Status** zeigt, wie der Sicherheitsbeauftragte das Zugriffsrechte erhalten hat:
  - **Geerbt** (blauer Text): Das Zugriffsrecht wurde von einem übergeordneten Knoten geerbt.
  - **Überschrieben** (brauner Text): Das Zugriffsrecht wurde von einem übergeordneten Knoten geerbt, jedoch am ausgewählten Knoten durch direkte Zuweisung überschrieben.
  - **Direkt zugewiesen** (schwarzer Text): Das Zugriffsrecht wurde direkt am ausgewählten Knoten zugewiesen.

  Für geerbte Rechte können Sie in der Spalte **Status** einen Tooltip anzeigen, der den Ursprung des relevanten Rechts zeigt.

11.11 Höherstufen von Sicherheitsbeauftragten

Sie haben folgende Möglichkeiten:

- Sie können einen Benutzer im Bereich **Benutzer & Computer** zum Sicherheitsbeauftragten ernennen.
- Sie können einen Sicherheitsbeauftragten im Bereich **Sicherheitsbeauftragte** zu einem Haupt-Sicherheitsbeauftragten ernennen.

11.11.1 Voraussetzungen für die Ernennung eines Benutzers zum Sicherheitsbeauftragten

Ein Sicherheitsbeauftragter mit den erforderlichen Rechten kann Benutzer zu Sicherheitsbeauftragten machen und ihnen Rollen zuweisen.

Auf diese Weise ernannte Sicherheitsbeauftragte können sich mit Ihren Windows-Anmeldeinformationen oder ihrer Token/Smartcard-PIN an das SafeGuard Management Center anmelden. Sie können genauso wie andere Sicherheitsbeauftragte agieren und verwaltet werden.

Folgende Voraussetzungen müssen erfüllt sein:

- Benutzer, die zu Sicherheitsbeauftragten ernannt werden sollen, müssen aus einem Active Directory importiert und im SafeGuard Management Center unter **Benutzer & Computer** sichtbar sein.

- Ein zum Sicherheitsbeauftragter ernannter Benutzer benötigt für die Anmeldung an das SafeGuard Management Center als Sicherheitsbeauftragter ein Benutzerzertifikat. Sie können dieses Zertifikat erstellen, wenn Sie den Benutzer zum Sicherheitsbeauftragten ernennen (siehe Ernennen eines Benutzers zum Sicherheitsbeauftragten (Seite 67)). Für die Anmeldung mit den Windows-Anmeldeinformationen muss die .p12-Datei mit dem privaten Schlüssel in der SafeGuard Enterprise Datenbank vorhanden sein. Für die Anmeldung mit Token bzw. Smartcard-PIN muss sich die .p12-Datei mit dem privaten Schlüssel auf dem Token bzw. der Smartcard befinden.

  Hinweis: Wenn Sie ein Zertifikat erstellen, wenn Sie einen Benutzer höher stufen, dann ist das Kennwort des Zertifikats für die Anmeldung am SafeGuard Management Center notwendig. Es ist das Kennwort des Zertifikats einzugeben, obwohl nach dem Windows Kennwort gefragt wird. Das ist auch der Fall bei der Anmeldung zum SafeGuard Enterprise Web Help Desk.

11.11.2 Ernennen eines Benutzers zum Sicherheitsbeauftragten

Voraussetzung: Um einen Benutzer zum Sicherheitsbeauftragten zu ernennen, müssen Sie ein Haupt-Sicherheitsbeauftragter oder ein Sicherheitsbeauftragter mit den erforderlichen Rechten sein.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie zum Sicherheitsbeauftragten machen möchten. Wählen Sie **Diesen Benutzer zum Sicherheitsbeauftragten machen**.
3. Der nächste Schritt richtet sich danach, ob für den ausgewählten Benutzer ein Benutzerzertifikat verfügbar ist.

   - Wurde dem Benutzer bereits ein Benutzerzertifikat zugewiesen, so wird der **Rollenauswahl** Dialog angezeigt. Fahren Sie mit Schritt 4 fort.

   - Ist kein Benutzerzertifikat verfügbar, so werden Sie in einer Meldung gefragt, ob für diesen Benutzer ein selbst-signiertes Schlüsselpaar erzeugt werden soll. Klicken Sie auf **Ja**, geben Sie im **Kennwort für neues Zertifikat** Dialog ein Kennwort ein und bestätigen Sie es. Nun wird der **Rollenauswahl** Dialog angezeigt.

4. Wählen Sie im **Rollenauswahl** Dialog die erforderlichen Rollen aus und klicken Sie auf **OK**.

Der Benutzer ist nun Sicherheitsbeauftragter und wird im Bereich **Sicherheitsbeauftragte** mit seinem Benutzernamen angezeigt. Die jeweiligen Eigenschaften lassen sich durch Auswahl des gewünschten Sicherheitsbeauftragten im Navigationsfenster anzeigen. Ist der private Schlüssel des Benutzers in der Datenbank gespeichert, so ist **Kein Token** aktiviert. Wenn sich der private Schlüssel auf dem Token oder der Smartcard befindet, ist **Optional** aktiviert.

Nach Wunsch können Sie den Sicherheitsbeauftragten per Drag&Drop auf der gewünschten Position in der Baumstruktur des Bereichs **Sicherheitsbeauftragte** platzieren.

Der Sicherheitsbeauftragte kann sich mit dem angezeigten Namen an das SafeGuard Management Center anmelden.

11.11.3 Ernennen eines Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten

Voraussetzung: Um einen Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten zu ernennen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten, den Sie zum Haupt-Sicherheitsbeauftragten ernennen möchten. Wählen Sie **Zum Haupt-Sicherheitsbeauftragten ernennen**.
3. Weist der ausgewählte Sicherheitsbeauftragte untergeordnete Sicherheitsbeauftragte auf, so werden Sie dazu aufgefordert, einen neuen übergeordneten Knoten für diese untergeordneten Sicherheitsbeauftragten auszuwählen.

Der Sicherheitsbeauftragte wird zum Haupt-Sicherheitsbeauftragten ernannt und unter dem Knoten **Haupt-Sicherheitsbeauftragte** angezeigt. Als Haupt-Sicherheitsbeauftragter erhält der ernannte Sicherheitsbeauftragte alle Rechte auf alle Objekte und verliert somit alle zugewiesenen Rollen sowie einzeln gewährte Domänen-Zugriffsberechtigungen im Bereich **Benutzer & Computer**.

11.12 Zurückstufen von ernannten Haupt-Sicherheitsbeauftragten

Voraussetzung: Nur Haupt-Sicherheitsbeauftragte können die Ernennung von Sicherheitsbeauftragten zu Haupt-Sicherheitsbeauftragten rückgängig machen.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Haupt-Sicherheitsbeauftragten, dessen Ernennung Sie rückgängig machen möchten. Wählen Sie **Zum Sicherheitsbeauftragten zurückstufen**.
3. Sie werden dazu aufgefordert, einen übergeordneten Knoten für den Sicherheitsbeauftragten zu wählen und mindestens eine Rolle zuzuweisen.

Die Ernennung des Sicherheitsbeauftragten zum Haupt-Sicherheitsbeauftragten wird rückgängig gemacht und der Sicherheitsbeauftragte wird unter dem ausgewählten **Sicherheitsbeauftragten** Knoten angezeigt. Der Sicherheitsbeauftragte verliert alle Rechte für alle Objekte und erhält nur die Rechte, die den zugewiesenen Rollen zugeordnet sind. Ein Sicherheitsbeauftragter, dessen Ernennung zum Haupt-Sicherheitsbeauftragten rückgängig gemacht wurde, hat zunächst keine Domänen-Zugriffsrechte. Domänen-Zugriffsrechte müssen einzeln im Bereich **Benutzer & Computer** in der Registerkarte **Zugriff** gewährt werden.

11.13 Ändern des Zertifikats eines Sicherheitsbeauftragten

Voraussetzung: Um das Zertifikat eines Sicherheitsbeauftragten oder Haupt-Sicherheitsbeauftragten zu ändern, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster auf den Sicherheitsbeauftragten, dessen Zertifikat Sie ändern möchten. Das aktuelle Zertifikat wird im Aktionsbereich auf der rechten Seite im Feld **Zertifikate** angezeigt.
3. Klicken Sie im Aktionsbereich auf die Dropdownliste **Zertifikate** und wählen Sie ein anderes Zertifikat aus.
4. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um Ihre Änderungen in der Datenbank zu speichern.

11.14 Anordnen von Sicherheitsbeauftragten in der Baumstruktur

Sicherheitsbeauftragte lassen sich im **Sicherheitsbeauftragte** Navigationsbereich des SafeGuard Management Center gemäß der Organisationsstruktur Ihres Unternehmens hierarchisch anordnen.

Die Baumstruktur lässt sich für alle Sicherheitsbeauftragten, außer für Haupt-Sicherheitsbeauftragte, ordnen. Haupt-Sicherheitsbeauftragte werden in einer nicht-hierarchischen Liste unter dem Haupt-Sicherheitsbeauftragten-Knoten angezeigt. Der Sicherheitsbeauftragten-Knoten enthält eine Baumstruktur, in der jeder Knoten einen Sicherheitsbeauftragten repräsentiert. Diese hierarchische Anordnung gibt jedoch keine Hierarchie in Bezug auf Rechte und Rollen wieder.

Voraussetzung: Um einen Sicherheitsbeauftragten in der Baumstruktur zu verschieben, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu modifizieren.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Ziehen Sie den gewünschten Sicherheitsbeauftragten im Navigationsfenster per Drag&Drop zum gewünschten Knoten.

Alle dem Sicherheitsbeauftragten untergeordneten Sicherheitsbeauftragte werden ebenfalls verschoben.

11.15 Schneller Wechsel zwischen Sicherheitsbeauftragten

Sie können das SafeGuard Management Center schnell und einfach neu starten, wenn Sie sich mit einem anderen Sicherheitsbeauftragten anmelden möchten.

1. Wählen Sie im SafeGuard Management Center **Datei > Sicherheitsbeauftragten wechseln**. Das SafeGuard Management Center wird neu gestartet und es wird ein Anmeldedialog angezeigt.
2. Wählen Sie den Sicherheitsbeauftragten, mit dem Sie sich an das SafeGuard Management Center anmelden möchten, und geben Sie das zugehörige Kennwort ein. Wenn Sie im Multi Tenancy Modus arbeiten, werden Sie wieder an dieselbe Datenbankkonfiguration angemeldet.

Das SafeGuard Management Center wird neu gestartet und zeigt die dem angemeldeten Sicherheitsbeauftragten zugeordnete Ansicht.

11.16 Löschen eines Sicherheitsbeauftragten

Voraussetzung: Um einen Sicherheitsbeauftragten zu löschen, benötigen Sie das Recht, Sicherheitsbeauftragte einzusehen und zu löschen.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf den Sicherheitsbeauftragten oder den Haupt-Sicherheitsbeauftragten, den Sie löschen möchten. Wählen Sie **Löschen**. Beachten Sie, dass Sie den Sicherheitsbeauftragten, mit dem Sie angemeldet sind, nicht löschen können.
3. Weist der ausgewählte Sicherheitsbeauftragte untergeordnete Sicherheitsbeauftragte auf, so werden Sie dazu aufgefordert, einen neuen übergeordneten Knoten für diese untergeordneten Sicherheitsbeauftragten auszuwählen.

Der Sicherheitsbeauftragte wird aus der Datenbank gelöscht.

Hinweis: Mindestens ein Haupt-Sicherheitsbeauftragter, der explizit als Beauftragter angelegt wurde und nicht nur zum Sicherheitsbeauftragten höhergestuft wurde, muss immer in der Datenbank verbleiben. Wird ein Benutzer, der zum Sicherheitsbeauftragten ernannt wurde, aus der Datenbank gelöscht, so wird auch sein Benutzerkonto aus der Datenbank gelöscht.

Hinweis: Wenn der zu löschende Sicherheitsbeauftragte eine Rolle hat, die zusätzliche Autorisierung umfasst und dem Sicherheitsbeauftragten als einziger diese Rolle zugewiesen ist, wird der Sicherheitsbeauftragte trotzdem gelöscht. Es wird angenommen, dass der Haupt-Sicherheitsbeauftragte die zusätzliche Autorisierung übernimmt.

12 Schlüssel und Zertifikate

SafeGuard Enterprise erzeugt in der Standardeinstellung beim Import der Verzeichnisstruktur automatisch Schlüssel für:

- Domänen
- Container/OUs

und weist diese den entsprechenden Objekten zu. Computer- und Benutzerschlüssel werden bei Bedarf erzeugt.

Schlüssel für Gruppen

In der Standardeinstellung erzeugt SafeGuard Enterprise nicht automatisch Schlüssel für Gruppen. Dieses Verhalten ist standardmäßig deaktiviert. All Sicherheitsbeauftragter können Sie dieses Verhalten in der **Schlüssel** Registerkarte ändern, indem Sie **Extras > Optionen** wählen. Ist in der **Schüssel** Registerkarte die Option **Gruppen** ausgewählt, so generiert SafeGuard Enterprise automatisch Gruppenschlüssel, wenn die Datenbank synchronisiert wird. In der Registerkarte **Synchronisierung**wird unten angegeben, für was Schlüssel bei der Durchführung der Synchronisierung erzeugt werden.

Schlüssel können nicht gelöscht werden! Sie sind immer in der SafeGuard Enterprise Datenbank enthalten.

Beim ersten Starten eines Endpoints erzeugt SafeGuard Enterprise einen Computerschlüssel für diesen Endpoint (definierter Computerschlüssel).

Hinweis: Der definierte Computerschlüssel wird nur dann erzeugt, wenn volume-basierende Verschlüsselung auf dem Endpoint installiert ist.

Bei der Anmeldung erhält jeder Benutzer alle Schlüssel aus seinem Schlüsselbund. Dieser Schlüsselbund besteht aus:

- aus den Schlüsseln der Gruppen, in denen der Benutzer Mitglied ist.
- aus den Schlüsseln der den Gruppen, in denen er Mitglied ist, übergeordneten Container/OUs.

Durch die Schlüssel in seinem Schlüsselbund ist festgelegt, auf welche Daten der Benutzer zugreifen kann. Es ist dem Benutzer nur möglich, auf Daten zuzugreifen, für die er den passenden Schlüssel besitzt.

Hinweis: Um zu vermeiden, dass zu viele nicht benutzte Schlüssel im Schlüsselring des Benutzers angezeigt werden, können Sie festlegen, dass Schlüssel ausgeblendet werden sollen. Weitere Informationen finden Sie unter Verbergen von Schlüsseln (Seite 73).

Alle vorhandenen Schlüssel werden angezeigt, wenn Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer** klicken und die Registerkarte **Schlüssel** wählen.

Alle überhaupt vorhandenen Schlüssel können angezeigt werden, wenn Sie im Navigationsbereich des SafeGuard Management Centers auf **Schlüssel und Zertifikate** klicken und **Schlüssel** wählen. Sie können Listen für **Zugewiesene Schlüssel** und **Inaktive Schlüssel** generieren.

Hinweis: Die Liste **Zugewiesene Schlüssel** zeigt nur die Schlüssel, die Objekten zugewiesen sind, für die Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** haben. In der Ansicht

Schlüssel wird die Anzahl an allen verfügbaren Schlüsseln ungeachtet Ihrer Zugriffsrechte angegeben. Die Liste **Zugewiesene Schlüssel** zeigt die Anzahl an Schlüsseln, die gemäß Ihren Zugriffsrechten sichtbar sind.

1. Diese Ansicht wird durch Klicken auf **Benutzer & Computer** geöffnet.
2. Die Schlüssel eines hier markierten Objekts werden im Aktionsbereich und in den dazugehörigen Ansichten angezeigt
3. Die Anzeige im Aktionsbereich ist abhängig von der Auswahl im Navigationsbereich. Es werden alle dem ausgewählten Objekt zugewiesenen Schlüssel angezeigt.
4. Unter **Verfügbare Schlüssel** werden alle verfügbaren Schlüssel angezeigt. Dem ausgewählten Objekt bereits zugewiesene Schlüssel sind ausgegraut. Über **Filter** kann zwischen bereits einem Objekt zugewiesenen (aktiven) und noch keinem Objekt zugewiesenen (inaktiven) Schlüsseln umgeschaltet werden.

Nach dem Import verfügt jeder Benutzer über eine Anzahl von Schlüsseln, die zur Datenverschlüsselung verwendet werden können.

12.1 Schlüssel für die Datenverschlüsselung

Benutzern können bestimmte Schlüssel zur Verschlüsselung von Volumes zugewiesen werden, indem Richtlinien vom Typ **Geräteschutz** angelegt werden.

In einer Richtlinie vom Typ **Geräteschutz** können Sie die Einstellung **Schlüssel für die Verschlüsselung** für jedes Medium festlegen.

Hier können Sie festlegen, welche Schlüssel der Benutzer bei der Verschlüsselung verwenden darf bzw. muss:

- **Beliebiger Schlüssel im Schlüsselring des Benutzers**

  Benutzer können nach der Anmeldung an Windows auswählen, welchen Schlüssel sie für die Verschlüsselung des Laufwerks verwenden möchten. Es wird ein Dialog angezeigt, in dem die Benutzer den gewünschten Schlüssel auswählen können.

- **Alle, außer persönliche Schlüssel im Schlüsselring**

  Benutzer dürfen ihren persönlichen Schlüssel nicht verwenden, um Daten zu verschlüsseln.

- **Beliebiger Gruppenschlüssel im Schlüsselring des Benutzers**

  Benutzer dürfen nur aus den in ihrem Schlüsselbund vorhandenen Gruppenschlüsseln auswählen.

- **Definierter Computerschlüssel**

  Der definierte Computerschlüssel ist der einzigartige Schlüssel, der von SafeGuard Enterprise nur für den jeweiligen Computer während des ersten Startvorgangs erzeugt wird. Der Benutzer hat keine Auswahlmöglichkeit. Ein definierter Computerschlüssel wird nur für die Boot- und Systempartition eingesetzt und für Laufwerke, auf denen sich Dokumente und Einstellungen befinden.

- **Definierter Schlüssel aus der Liste**

  Diese Option erlaubt es Ihnen, einen bestimmten Schlüssel zu definieren, der vom Benutzer zur Verschlüsselung verwendet werden muss. Wenn Sie dem Benutzer einen Schlüssel auf diese Weise vorgeben wollen, müssen Sie unter **Für Verschlüsselung definierter**

Schlüssel einen Schlüssel festlegen. Diese Option wird erst angezeigt, wenn Sie D**efinierter Schlüssel aus der Liste** ausgewählt haben.

Wenn Sie auf die **[...]** Schaltfläche neben der Option **Für Verschlüsselung definierter Schlüssel** klicken, wird ein Dialog angezeigt, in dem Sie einen Schlüssel angeben können. Stellen Sie sicher, dass der Benutzer auch den entsprechenden Schlüssel hat.

Markieren Sie den gewünschten Schlüssel und klicken Sie auf **OK**. Der ausgewählte Schlüssel wird auf dem Endpoint-Computer zur Verschlüsselung verwendet.

12.1.1 Zuweisen von Schlüsseln im Bereich Benutzer & Computer

Um Schlüssel zuzuweisen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für das relevante Objekt.

So weisen Sie Benutzern neue Schlüssel zu:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsbereich das gewünschte Objekt aus (z. B. Benutzer, Gruppe oder Container).
3. Klicken Sie mit der rechten Maustaste auf die Registerkarte **Schlüssel** und wählen Sie **Neuen Schlüssel zuweisen** aus dem Kontextmenü.
4. Führen Sie im Dialog **Neuen Schlüssel zuweisen** folgende Aufgaben aus:
   a) Geben Sie einen **Symbolischen Namen** und eine **Beschreibung** für den Schlüssel ein.
   b) Um den Schlüssel im Schlüsselring des Benutzers zu verbergen, wählen Sie das Kontrollkästchen **Schlüssel verbergen**.
5. Klicken Sie auf **OK**.

Der Schlüssel wird zugewiesen und in der **Schlüssel** Registerkarte angezeigt.

12.1.2 Verbergen von Schlüsseln

Um zu vermeiden, das zu viele nicht benutzte Schlüssel im Schlüsselring des Benutzers auf dem Endpoint angezeigt werden, können Sie festlegen, dass Schlüssel ausgeblendet werden sollen. Schlüssel, die nicht im Schlüsselring des Benutzers angezeigt werden, können trotzdem noch für den Zugriff auf verschlüsselte Dateien benutzt werden. Sie können jedoch nicht für das Verschlüsseln neuer Dateien verwendet werden.

So verbergen Sie Schlüssel:

1. Klicken Sie im SafeGuard Management Center auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsbereich auf **Schlüssel** und wählen Sie **Zugewiesene Schlüssel**.

   Das Fenster **Zugewiesene Schlüssel** mit der Spalte **Schlüssel verbergen** wird angezeigt.
3. Hier gibt es zwei Möglichkeiten:
   - Wählen Sie das Kontrollkästchen **Schlüssel verbergen** für den gewünschten Schlüssel.
   - Wählen Sie einen oder mehrere Schlüssel aus und öffnen Sie das Kontextmenü per Rechtsklick.

     Wählen Sie **Schlüssel vor Benutzer verbergen**.
4. Speichern Sie Ihre Änderungen in der Datenbank.

Die angegebenen Schlüssel werden nicht im Schlüsselring des Benutzers angezeigt.

Weitere Informationen zum Anzeigen des Schlüsselrings des Benutzers auf dem Endpoint finden Sie in der *SafeGuard Enterprise Benutzerhilfe* im Kapitel *System Tray Icon und Balloon-Ausgabe*.

Hinweis: Wenn in einer Richtlinie ein verborgener Schlüssel für die Verschlüsselung festgelegt ist, hat die Einstellung **Schlüssel verbergen** keine Auswirkungen auf die Verschlüsselung auf dem Endpoint.

12.2 Persönliche Schlüssel für die dateibasierende Verschlüsselung mit File Encryption

Ein persönlicher Schlüssel ist eine besondere Art von Verschlüsselungschlüssel, der für einen bestimmten Benutzer erzeugt wird und nicht mit anderen Benutzern gemeinsam verwendet werden kann. Ein persönlicher Schlüssel, der für einen bestimmten Benutzer aktiv ist, wird als aktiver persönlicher Schlüssel bezeichnet. Aktive persönliche Schlüssel können anderen Benutzern nicht zugewiesen werden.

In **File Encryption** Richtlinien können Sie Verschlüsselungsregeln mit dem Platzhalter **Persönlicher Schlüssel** statt eines Schlüsselnamens definieren. Für solche Regeln wird als Verschlüsselungsschlüssel der aktive persönliche Schlüssel des Benutzers verwendet.

Wenn Sie eine Verschlüsselungsregel für den Pfad *C:\encrypt* für die Verschlüsselung mit dem persönlichen Schlüssel definieren, werden für die einzelnen Benutzer unterschiedliche Schlüssel verwendet. So können Sie sicherstellen, dass die Informationen in spezifischen Ordnern für die Benutzer privat sind. Weitere Informationen finden Sie unter Dateiverschlüsselung (Seite 181).

Wenn eine File Encryption Verschlüsselungsregel einen persönlichen Schlüssel für die Verschlüsselung vorsieht, werden für die relevanten Benutzer automatisch persönliche Schlüssel erzeugt, wenn sie noch keine aktiven persönlichen Schlüssel haben.

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie persönliche Schlüssel für ausgewählte Benutzer oder alle Benutzer in ausgewählten Gruppen im SafeGuard Management Center erzeugen. Sie können aktive persönliche Schlüssel auch zurückstufen, wenn zum Beispiel ein Benutzer das Unternehmen verlässt.

12.2.1 Automatisches Erzeugen von persönlichen Schlüsseln

Wenn eine File Encryption Verschlüsselungsregel einen persönlichen Schlüssel für die Verschlüsselung vorsieht und der Benutzer noch keinen aktiven persönlichen Schlüssel hat, erzeugt der SafeGuard Enterprise Server diesen automatisch. Nach Eingang der Richtlinie auf dem Endpoint kann der Benutzer so lange keine neuen Dateien in den von der File Encryption Verschlüsselungsregel abgedeckten Ordner anlegen, bis der erforderliche aktive persönliche Schlüssel verfügbar wird.

Wenn Sie zum ersten Mal **File Encryption**-Richtlinien mit Verschlüsselungsregeln mithilfe persönlicher Schlüssel auf eine größere Gruppe von Benutzern (mehrere hundert oder mehr) anwenden, die noch keine aktiven persönlichen Schlüssel haben, empfehlen wir, persönliche Schlüssel im SafeGuard Management Center zu erzeugen (siehe Erzeugen von persönlichen Schlüsseln für mehrere Benutzer (Seite 75)). Dies reduziert die Auslastung des SafeGuard Enterprise Servers.

12.2.2 Erzeugen eines persönlichen Schlüssels für einzelne Benutzer

Um einen persönlichen Schlüssel zu erzeugen, benötigen Sie die Rechte **Schlüssel erzeugen** und **Schlüssel zuweisen**. Darüber hinaus benötigen Sie das Zugriffsrecht **Voller Zugriff** für das relevante Objekt. Um einen aktiven persönlichen Schlüssel zu ersetzen, benötigen Sie das Recht **Persönliche Schlüssel verwalten**.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsbereich den gewünschten Benutzer.
3. Klicken Sie mit der rechten Maustaste auf die Registerkarte **Schlüssel** und wählen Sie **Neuen Schlüssel zuweisen** aus dem Kontextmenü.
4. Führen Sie im Dialog **Neuen Schlüssel zuweisen** folgende Aufgaben aus:
   a) Geben Sie eine Beschreibung für den persönlichen Schlüssel ein.
   b) Um den persönlichen Schlüssel im Schlüsselring des Benutzers zu verbergen, wählen Sie **Schlüssel verbergen**.
5. Abhängig davon, ob Sie einen persönlichen Schlüssel für einen Benutzer erzeugen, der bereits eine aktiven persönlichen Schlüssel hat, oder für einen Benutzer ohne einen solchen Schlüssel, zeigt der Dialog **Neuen Schlüssel zuweisen** verschiedene Kontrollkästchen. Wählen Sie das jeweils angezeigte Kontrollkästchen, um den neuen Schlüssel als persönlichen Schlüssel zu definieren:
   - **Persönlicher Schlüssel**: Dieses Kontrollkästchen wird für Benutzer angezeigt, die noch keinen aktiven persönlichen Schlüssel haben.
   - **Aktiven persönlichen Schlüssel ersetzen**: Dieses Kontrollkästchen wird für Benutzer angezeigt, die bereits einen aktiven persönlichen Schlüssel haben.
6. Klicken Sie auf **OK**.

Der persönliche Schlüssel wird für den ausgewählten Benutzer erzeugt. In der Registerkarte **Schlüssel** wird der Schlüssel als **Aktiver persönlicher Schlüssel** für den Benutzer angezeigt. Bei Benutzern, die bereits einen aktiven persönlichen Schlüssel hatten, wird der vorhandene Schlüssel zurückgestuft und der Benutzer erhält einen neuen. Der zurückgestufte persönliche Schlüssel verbleibt im Schlüsselring des Benutzers. Der aktive persönlichen Schlüssel kann anderen Benutzern nicht zugewiesen werden.

12.2.3 Erzeugen von persönlichen Schlüsseln für mehrere Benutzer

Um persönliche Schlüssel zu erzeugen, benötigen Sie die Rechte **Schlüssel erzeugen** und **Schlüssel zuweisen**. Darüber hinaus benötigen Sie das Zugriffsrecht **Voller Zugriff** für alle beteiligten Objekte. Um aktive persönliche Schlüssel zu ersetzen, benötigen Sie das Recht **Persönliche Schlüssel verwalten**.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie im Navigationsbereich mit der rechten Maustaste auf den Knoten, für den Sie persönliche Schlüssel erzeugen möchten:
   - Auf einen Domänenknoten,
   - auf den .Automatisch registriert Knoten im Stammverzeichnis oder in Domänen oder
   - auf einen Organisationseinheitenknoten.
3. Wählen Sie aus dem Kontextmenü den Befehl **Persönliche Schlüssel für Benutzer erzeugen**.

4. Führen Sie im Dialog **Persönliche Schlüssel für Benutzer erzeugen** folgende Schritte durch:
   a) Geben Sie eine Beschreibung für die persönlichen Schlüssel ein.
   b) Um die persönlichen Schlüssel im Schlüsselring der Benutzer zu verbergen, wählen Sie **Schlüssel verbergen**.
   c) Um vorhandene, aktive Schlüssel durch neue zu ersetzen, wählen Sie **Vorhandene, aktive persönliche Schlüssel ersetzen**.
5. Klicken Sie auf **OK**.

Für alle Benutzer im ausgewählten Knoten werden persönliche Schlüssel erzeugt. In der Registerkarte **Schlüssel** werden die Schlüssel als **Aktive persönliche Schlüssel** für die Benutzer angezeigt. Wenn Benutzer bereits zuvor einen aktiven persönlichen Schlüssel hatten und Sie **Vorhandene, aktive persönliche Schlüssel ersetzen** gewählt haben, werden die vorhandenen Schlüssel zurückgestuft und die Benutzer erhalten neue. Die zurückgestuften persönlichen Schlüssel verbleiben in den Schlüsselringen der Benutzer. Die einzelnen aktiven persönlichen Schlüssel können anderen Benutzern nicht zugewiesen werden.

12.2.4 Zurückstufen von aktiven persönlichen Schlüsseln

Um aktive persönliche Schlüssel zurückzustufen, benötigen Sie die Rechte **Schlüssel ändern** und **Persönliche Schlüssel verwalten**. Das Recht **Persönliche Schlüssel verwalten** ist standardmäßig der vordefinierten Rolle des Haupt-Sicherheitsbeauftragten (Master Security Officer) zugewiesen. Es kann jedoch auch neuen, benutzerdefinierten Rollen zugewiesen werden. Darüber hinaus benötigen Sie das Zugriffsrecht **Voller Zugriff** für das relevante Objekt.

Sie können aktive persönliche Schlüssel manuell zurückstufen, wenn zum Beispiel ein Benutzer das Unternehmen verlässt. Wenn Sie das Recht **Persönliche Schlüssel verwalten** haben, können Sie den zurückgestuften persönlichen Schlüssel dieses Benutzers anderen Benutzern zuweisen, um Ihnen Lesezugriff auf Dateien zu gewähren, die mit diesem Schlüssel verschlüsselt sind. Der Schlüssel kann jedoch nicht zum Verschlüsseln von Dateien verwendet werden.

Hinweis: Dieser Vorgang kann nicht rückgängig gemacht werden. Ein zurückgestufter persönlicher Schlüssel kann nicht mehr als aktiver persönlicher Schlüssel verwendet werden, egal für welchen Benutzer.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsbereich den gewünschten Benutzer.
3. Klicken Sie in der Registerkarte **Schlüssel** mit der rechten Maustaste auf den gewünschten **Aktiven persönlichen Schlüssel** und wählen Sie **Persönlichen Schlüssel zurückstufen** aus dem Kontextmenü.

Der Schlüssel wird zurückgestuft. Er ist immer noch ein persönlicher Schlüssel, kann jedoch nicht mehr als aktiver persönlicher Schlüssel verwendet werden. Wenn eine File Encryption Verschlüsselungsregel den persönlichen Schlüssel für die Verschlüsselung vorsieht und der Benutzer keinen aktiven persönlichen Schlüssel hat, erzeugt der SafeGuard Enterprise Server diesen automatisch.

12.3 Zertifikate

- Einem Benutzer kann jeweils nur ein Zertifikat zugewiesen sein. Wenn dieses Benutzerzertifikat auf einem Token gespeichert ist, können die Benutzer sich nur mit diesem Token (kryptographischer Token - Kerberos) an ihrem Endpoint anmelden.

- Beachten Sie, dass beim Importieren eines Benutzerzertifikats sowohl der öffentliche als auch der private Bereich des Zertifikats importiert werden. Wird nur der öffentliche Bereich importiert, so wird nur die Anmeldung mit Token unterstützt.
- Die Kombination aus CA Zertifikaten und CRL (Certificate Revocation List) Zertifikaten muss übereinstimmen. Andernfalls können sich die Benutzer nicht an den entsprechenden Endpoints anmelden. Bitte überprüfen Sie, ob die Kombination korrekt ist. SafeGuard Enterprise übernimmt diese Überprüfung nicht!
- Wenn Certification Authority (CA) Zertifikate in der Datenbank gelöscht werden und Sie diese nicht mehr verwenden möchten, sollten Sie diese Zertifikate manuell aus dem lokalen Speicher aller Administrator-Computer entfernen.

  SafeGuard Enterprise kann dann nur mit ablaufenden Zertifikaten umgehen, wenn der alte und neue private Schlüssel auf demselben Token stehen.
- CA-Zertifikate können nicht von einem Token entnommen und in der Datenbank oder im Zertifikatsspeicher gespeichert werden. Wenn Sie CA-Zertifikate verwenden möchten, müssen diese in Dateiform zur Verfügung stehen, nicht nur auf einem Token. Dies gilt auch für CRLs.
- Von SafeGuard Enterprise generierte Zertifikate sind mit SHA-1 oder SHA-256 zur Verifizierung signiert. SHA-256 bietet erweiterte Sicherheit und wird standardmäßig für Erstinstallationen benutzt. Wenn noch die Verwaltung von SafeGuard Enterprise 6 Endpoints oder älteren Endpoints notwendig ist, wird standardmäßig SHA-1 benutzt.
- Zertifikate, die vom Kunden zur Verfügung gestellt und in SafeGuard Enterprise importiert werden, werden derzeit nicht gemäß RFC3280 verifiziert. So wird z. B. nicht verhindert, dass Signatur-Zertifikate für Verschlüsselungszwecke benutzt werden.
- Die Anmeldezertifikate für Sicherheitsbeauftragte müssen sich im “MY” Zertifikatspeicher befinden.

Hinweis: Die Liste **Zugewiesene Zertifikate** unter **Schlüssel und Zertifikate** zeigt nur die Zertifikate, die Objekten zugewiesen sind, für die Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** haben. In der Ansicht **Zertifikat** wird die Anzahl an allen verfügbaren Zertifikaten ungeachtet Ihrer Zugriffsrechte angegeben. Die Liste **Zugewiesene Zertifikate** zeigt die Anzahl an Zertifikaten, die gemäß Ihren Zugriffsrechten sichtbar sind.

Um Zertifikate zu ändern, benötigen Sie das Zugriffsrecht **Voller Zugriff** für den Container, in dem sich der Benutzer befindet.

12.3.1 Importieren von CA-Zertifikaten und Certificate Revocation Lists

Wenn CA-Zertifikate verwendet werden, importieren Sie die vollständige CA-Hierarchie einschließlich aller CRLs in die SafeGuard-Datenbank. CA-Zertifikate können nicht von Token entnommen werden. Diese Zertifikate müssen als Dateien zur Verfügung stehen, damit Sie sie in die SafeGuard Enterprise Datenbank importieren können. Dies gilt auch für Certificate Revocation Lists (CRL).

1. Klicken Sie im SafeGuard Management Center auf **Schlüssel & Zertifikate**.
2. Wählen Sie **Zertifikate** und klicken Sie auf das **CA-Zertifikate importieren** Symbol in der Symbolleiste. Suchen Sie die CA-Zertifikatsdateien, die Sie importieren möchten.

   Die importierten Zertifikate werden im rechten Aktionsbereich angezeigt.

3. Wählen Sie **Zertifikate** und klicken Sie auf das **CRL importieren** Symbol in der Symbolleiste. Suchen Sie die CRL-Dateien, die Sie importieren möchten.

   Die importierten CRLs werden im rechten Aktionsbereich angezeigt.

4. Überprüfen Sie, ob CA und CRL korrekt sind und übereinstimmen. Die Kombination von CA-Zertifikaten und CRL zusammenpassen, da ansonsten eine Anmeldung an allen betroffenen Computern nicht mehr möglich ist. SafeGuard Enterprise übernimmt diese Überprüfung nicht.

12.3.2 Ändern des Algorithmus für selbst-signierte Zertifikate

Voraussetzungen: Alle SafeGuard Enterprise Komponenten müssen die Version 6.1 oder höher haben.

Von SafeGuard Enterprise erzeugte Zertifikate, zum Beispiel Unternehmens-, Maschinen-, Sicherheitsbeauftragten- und Benutzerzertifikate, sind bei einer Erstinstallation standardmäßig zur Erweiterung der Sicherheit mit dem Hash-Algorithmus **SHA-256** signiert.

Bei der Aktualisierung von SafeGuard Enterprise 6 oder einer früheren Version wird für selbst-signierte Zertifikate automatisch der Hash-Algorithmus **SHA-1** benutzt. Nach Abschluss der Aktualisierung können Sie den Hash-Algorithmus für erweiterte Sicherheit manuell zu **SHA-256** ändern.

Hinweis: Ändern Sie den Algorithmus nur dann zu **SHA-256**, wenn bei allen SafeGuard Enterprise Komponenten und Endpoints eine Aktualisierung auf die aktuelle Version durchgeführt wurde. In gemischten Umgebungen, in denen zum Beispiel SafeGuard Enterprise 6 Endpoints mit dem SafeGuard Management Center 7 verwaltet werden, wird **SHA-256** nicht unterstützt. Wenn Sie eine gemischte Umgebung benutzen, dürfen Sie diesen Vorgang nicht ausführen. In diesem Fall dürfen Sie den Algorithmus nicht zu **SHA-256** ändern.

Zum Ändern des Algorithmus für selbst-signierte Zertifikate müssen Sie folgende Handlungsschritte ausführen:

- Ändern des Hash-Algorithmus
- Erzeugen einer Certificate Change Order (CCO)
- Erzeugen eines Konfigurationspakets mit der CCO
- Neustart der SafeGuard Enterprise (Datenbank-) Server
- Verteilen und Installieren der Konfigurationspakete auf den Endpoints

So ändern Sie den Algorithmus für selbst-signierte Zertifikate:

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wählen Sie in der Registerkarte **Allgemein** unter **Zertifikate** den erforderlichen Algorithmus in **Hash-Algorithmus für erzeugte Zertifikate** aus und klicken Sie auf **OK**.
3. Klicken Sie in der Registerkarte **Zertifikate** unter **Anforderung** auf **Aktualisieren**. Geben Sie im Dialog **Unternehmenszertifikat aktualisieren** einen Namen für die CCO an und legen Sie einen Backup-Pfad fest. Geben Sie ein Kennwort für die P12-Datei ein und bestätigen Sie Ihre Eingabe. Geben Sie nach Wunsch eine Anmerkung ein und klicken Sie auf **Erzeugen**.
4. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass diese Änderung nicht rückgängig gemacht werden kann und dass alle nachfolgend erstellten Konfigurationspakete diese CCO enthalten müssen, damit Sie auf bereits installierten Endpoints wirksam werden können.

5. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass die Aktualisierung erfolgreich war und dass eine CCO erzeugt wurde, die in alle Konfigurationspakete aufgenommen werden soll. Klicken Sie auf **OK**.
6. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.
7. Wählen Sie den erforderlichen Konfigurationspakettyp: **Pakete für Managed Clients** oder **Pakete für Standalone Clients**.
8. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen Ihrer Wahl für das Konfigurationspaket ein.
9. Wählen Sie die zuvor erstellte **CCO**.
10. Treffen Sie je nach Anforderung eine zusätzliche Auswahl.
11. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
12. Klicken Sie auf **Konfigurationspaket erstellen**.

    Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt.

13. Starten Sie alle SafeGuard Enterprise (Datenbank-) Server neu.
14. Verteilen Sie das Paket an die durch SafeGuard Enterprise geschützten Endpoints zur Installation.

Alle durch SafeGuard Enterprise generierten Zertifikate werden mit dem neuen Algorithmus signiert.

Siehe auch http://www.sophos.com/de-de/support/knowledgebase/116791.aspx.

12.4 Exportieren des Unternehmenszertifikats und des Zertifikats des Haupt-Sicherheitsbeauftragten

In einer SafeGuard Enterprise Installation sind die beiden folgenden Elemente von entscheidender Bedeutung und erfordern daher die Erstellung von Backups an einem sicheren Speicherort:

- das in der SafeGuard-Datenbank gespeicherte Unternehmenszertifikat
- das Zertifikat des Haupt-Sicherheitsbeauftragten (MSO) im Zertifikatsspeicher des Computers, auf dem das SafeGuard Management Center installiert ist.

Beide Zertifikate lassen sich als .p12 Dateien zur Erstellung von Sicherungskopien exportieren. Um Installationen wiederherzustellen, können Sie die relevanten Unternehmens- und Sicherheitsbeauftragtenzertifikate als .p12 Dateien importieren und Sie beim Einrichten einer neuen Datenbank benutzen. Dadurch vermeiden Sie das Wiederherstellen der gesamten Datenbank.

Hinweis: Wir empfehlen, diesen Vorgang direkt nach der Erstkonfiguration des SafeGuard Management Centers auszuführen.

12.4.1 Exportieren von Unternehmenszertifikaten

Hinweis: Nur Haupt-Sicherheitsbeauftragte sind dazu berechtigt, Unternehmenszertifikate zur Erstellung eines Backups zu exportieren.

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **Unternehmenszertifikat** auf **Exportieren**.

3. Sie werden aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Unternehmenszertifikat wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

12.4.2 Exportieren des Zertifikats des Haupt-Sicherheitsbeauftragten

So erstellen Sie ein Backup des Zertifikats des derzeit am SafeGuard Management Center angemeldeten Haupt-Sicherheitsbeauftragten:

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wählen Sie die Registerkarte **Zertifikate** und klicken Sie im Bereich **<Administrator> Zertifikat** auf **Exportieren**.
3. Sie werden aufgefordert, ein Kennwort für die Sicherung der exportierten Datei einzugeben. Geben Sie ein Kennwort ein, bestätigen Sie es und klicken Sie auf **OK**.
4. Geben Sie einen Dateinamen und einen Speicherort für die zu exportierende Datei ein und klicken Sie auf **OK**.

Das Zertifikat des derzeit angemeldeten Haupt-Sicherheitsbeauftragten wird als P12-Datei an den definierten Speicherort exportiert und kann für Recovery-Vorgänge benutzt werden.

12.5 Virtuelle Clients

Hinweis: Virtuelle Clients können nur für **SafeGuard full disk encryption with SafeGuard Power-on Authentication (POA)** verwendet werden.

Virtuelle Clients sind spezifische verschlüsselte Schlüsseldateien, die im Rahmen eines Challenge/Response-Verfahrens für Recovery-Zwecke verwendet werden können, wenn die benötigten Benutzerinformationen nicht zur Verfügung stehen und ein Challenge/Response-Verfahren normalerweise nicht möglich wäre (z. B. bei beschädigter SafeGuard POA).

Um in dieser komplexen Recovery-Situation ein Challenge/Response-Verfahren zu ermöglichen, lassen sich spezifische Dateien, die als virtuelle Clients bezeichnet werden, erstellen. Diese Dateien müssen vor dem Challenge/Response-Verfahren an den Benutzer verteilt werden. Mit virtuellen Clients lasst sich ein Challenge/Response-Verfahren mit einem Schlüssel-Recovery Tool auf dem Endpoint-Computer starten. Der Benutzer muss dann nur den Helpdesk-Beauftragten über den/die benötigten Schlüssel informieren und den Response-Code eingeben, um wieder Zugriff auf die verschlüsselten Volumes zu erhalten.

Der Zugriff kann entweder mit Hilfe eines einzelnen Schlüssels oder mit Hilfe einer verschlüsselten Schlüsseldatei, die mehrere Schlüssel enthält, wiederhergestellt werden.

Im Bereich **Schlüssel und Zertifikate** des SafeGuard Management Centers haben Sie folgende Möglichkeiten:

- Virtuelle Clients anlegen und exportieren
- Verschlüsselte Schlüsseldateien mit mehreren Schlüsseln anlegen und exportieren
- Virtuelle Clients und exportierte Schlüsseldateien anzeigen lassen und filtern
- Virtuelle Clients löschen

12.5.1 Anlegen von virtuellen Clients

Virtuelle Clients können für verschiedene Computer und in mehreren Challenge/Response-Verfahren benutzt werden.

1. Klicken Sie im SafeGuard Management Center auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie in der Symbolleiste auf **Virtuellen Client hinzufügen**.
4. Geben Sie einen eindeutigen Namen für den virtuellen Client ein und klicken Sie auf **OK**.

   Die virtuellen Clients werden anhand der hier eingegebenen Namen in der Datenbank identifiziert.

5. Klicken Sie auf das **Speichern** Symbol in der Symbolleiste, um den virtuellen Client in der Datenbank zu speichern.

Der neue virtuelle Client wird im Aktionsbereich angezeigt.

12.5.2 Export von virtuellen Clients

Nach dem Anlegen des virtuellen Client muss dieser in eine Datei exportiert werden. Diese Datei hat immer die Bezeichnung **`recoverytoken.tok`** und muss an den Helpdesk verteilt werden. Beim Starten eines Challenge/Response-Verfahrens über ein Recovery Tool, z. B. bei einer beschädigten SafeGuard POA, muss diese Datei in der Endpoint-Umgebung zur Verfügung stehen. Der Benutzer muss die Datei **`recoverytoken.tok`** im selben Verzeichnis ablegen, in dem sich auch das Recovery Tool befindet, damit ein Challenge/Response-Verfahren unterstützt wird.

1. Klicken Sie im SafeGuard Management Center auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie im Aktionsbereich auf das Lupensymbol, um nach dem gewünschten virtuellen Client zu suchen. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client exportieren**.
5. Wählen Sie einen Speicherort für die Datei **`recoverytoken.tok`** und klicken Sie auf **OK**. Eine entsprechende Meldung wird angezeigt.
6. Verteilen Sie die virtuelle Client-Datei **`recoverytoken.tok`** an die betreffenden SafeGuard Enterprise Benutzer.

Der Benutzer sollte diese Datei an einem sicheren Speicherort speichern, z. B. auf einem USB-Stick. Beim Starten eines Challenge/Response-Verfahrens muss diese Datei im selben Verzeichnis wie das Recovery Tool abgelegt sein.

12.5.3 Anlegen und Exportieren von Schlüsseldateien für den Recovery-Vorgang

Sind mehrere Schlüssel erforderlich, um den Zugriff auf ein verschlüsseltes Volume im Rahmen eines Recovery-Verfahrens mit virtuellen Clients wiederherzustellen, so kann der Sicherheitsbeauftragte diese Schlüssel in einer exportierten Schlüsseldatei zusammenfassen. Diese Schlüsseldatei wird mit einem Zufallskennwort verschlüsselt, das in der Datenbank gespeichert wird. Das Kennwort ist für jede angelegte Schlüsseldatei einzigartig.

Die verschlüsselte Schlüsseldatei muss an den Benutzer übertragen werden und ihm beim Starten eines Challenge/Response-Verfahrens über ein Recovery Tool zur Verfügung stehen.

Im Rahmen des Challenge/Response-Verfahrens wird das Kennwort für die Schlüsseldatei mit dem Response-Code übertragen. Die Schlüsseldatei kann daraufhin mit dem Kennwort entschlüsselt werden und es besteht wieder Zugriff auf alle Volumes, die mit den verfügbaren Schlüsseln verschlüsselt sind.

Um Schüsseldateien zu exportieren, benötigen Sie das Zugriffsrecht **Voller Zugriff** für die Objekte, denen die relevanten Schlüssel zugewiesen sind.

1. Klicken Sie im SafeGuard Management Center auf **Schlüssel & Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite zunächst auf **Virtuelle Clients** und dann auf **Exportierte Schlüsseldateien**.
3. Klicken Sie in der Symbolleiste auf **Schlüssel in eine Schlüsseldatei exportieren**.
4. Geben Sie im Dialog **Schlüssel in eine Schlüsseldatei exportieren** folgende Informationen ein:
   a) **Verzeichnis**: Klicken Sie auf **[...]**, um einen Speicherort für die Schlüsseldatei auszuwählen.
   b) **Dateiname**: Die Schlüsseldatei ist mit einem Zufallskennwort verschlüsselt, das hier angezeigt wird. Sie können den hier angezeigten Namen nicht ändern.
   c) Klicken Sie auf **Schlüssel hinzufügen** oder **Schlüssel entfernen**, um Schlüssel hinzuzufügen oder zu entfernen. Ein Popup-Fenster, in dem Sie nach den gewünschten Schlüsseln suchen und diese auswählen können, wird angezeigt. Klicken Sie auf **OK**, um die Auswahl zu bestätigen.
   d) Klicken Sie auf **OK**, um Ihre Angaben zu bestätigen.
5. Verteilen Sie diese Schlüsseldatei an die betreffende Endpoint-Umgebung. Sie muss vor der Eingabe des Response-Codes auf dem Endpoint zur Verfügung stehen.

12.5.4 Virtuelle Clients anzeigen und Ansicht filtern

Um Ihnen das Auffinden des erforderlichen virtuellen Clients oder Schlüssels während eines Challenge/Response-Verfahrens zu erleichtern, bietet der Bereich **Schlüssel und Zertifikate** des SafeGuard Management Centers verschiedene Filter- und Suchfunktionalitäten.

12.5.5 Ansichten für virtuelle Clients

1. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
2. Klicken Sie auf das Lupensymbol, um eine vollständige Liste aller virtuellen Clients zu erstellen.
3. Filtern Sie die virtuellen Clients nach **Symbolischer Name** oder **Schlüssel-GUID**.

12.5.6 Ansichten für exportierte Schlüsseldateien

1. Klicken Sie im SafeGuard Management Center zunächst auf **Virtuelle Clients** und dann auf **Exportierte Schlüsseldateien**.
2. Klicken Sie auf das Lupensymbol, um eine vollständige Liste aller exportierten Schlüsseldateien zu erstellen.
3. Klicken Sie auf das **+** Symbol neben der gewünschten Schlüsseldatei, um die in der Datei enthaltenen Schlüssel anzuzeigen.

12.5.7 Löschen von virtuellen Clients

1. Öffnen Sie das SafeGuard Management Center und klicken Sie auf **Schlüssel und Zertifikate**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Virtuelle Clients**.
3. Klicken Sie im Aktionsbereich auf das Lupensymbol, um nach dem gewünschten virtuellen Client zu suchen. Die verfügbaren virtuellen Clients werden angezeigt.
4. Wählen Sie den gewünschten Eintrag im Aktionsbereich aus und klicken Sie in der Symbolleiste auf **Virtuellen Client löschen**.
5. Speichern Sie ihre Änderungen in der Datenbank, indem Sie in der Symbolleiste auf das Symbol **Speichern** klicken.

Der virtuelle Client wird aus der Datenbank gelöscht.

13 Company Certificate Change Orders

Company Certificate Change Orders (CCOs) werden in folgenden Fällen verwendet:

- **Zum Erneuern des Unternehmenszertifikats**, wenn dieses bald abläuft.

  Die Erneuerung des Unternehmenszertifikats ist für zentral verwaltete Endpoints und Standalone-Endpoints möglich. Der Vorgang kann jedoch nur von der Management-Konsole aus ausgelöst werden.

- **Zum Verschieben von Standalone-Endpoints in eine andere Umgebung**, wenn Sie zum Beispiel zwei verschiedene Sophos SafeGuard Umgebungen haben und Sie diese in eine Sophos SafeGuard Umgebung zusammenführen möchten. Eine der beiden Umgebungen muss hier jeweils die Ziel-Umgebung sein.

  Hierzu wird das Unternehmenszertifikat der Endpoints einer Umgebung durch das Unternehmenszertifikat der Zielumgebung ausgetauscht.

  Hinweis: Nur Haupt-Sicherheitsbeauftragte sind zum Erzeugen von CCOs berechtigt. Um andere Sicherheitsbeauftragte dazu zu berechtigen, CCOs zu erzeugen, muss der Hauptsicherheitsbeauftragte eine benutzerdefinierte Rolle erstellen und dieser das Recht **CCOs verwalten** zuweisen.

13.1 Erneuern des Unternehmenszertifikats

Ein Unternehmenszertifikat, das bald abläuft, kann im SafeGuard Management Center erneuert werden. Sechs Monate vor Ablauf des Unternehmenszertifikat wird bei jeder Anmeldung an das SafeGuard Management Center eine Warnung angezeigt. Ohne gültiges Unternehmenszertifikat können Endpoints keine Verbindung mit dem Server herstellen. Die Erneuerung des Unternehmenszertifikats erfolgt in drei Schritten:

- Erzeugen einer Certificate Change Order (CCO)
- Erzeugen eines Konfigurationspakets mit der CCO
- Neustart der Server und Verteilen der Konfigurationspakete an die Endpoints

So erneuern Sie das Unternehmenszertifikat:

1. Wählen Sie **Extras > Optionen** in der SafeGuard Management Center Menüleiste.
2. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **Anforderung** auf **Aktualisieren**.
3. Geben Sie im Dialog **Unternehmenszertifikat aktualisieren** einen Namen für die CCO an und legen Sie einen Backup-Pfad fest. Geben Sie ein Kennwort für die P12-Datei ein und bestätigen Sie Ihre Eingabe. Geben Sie nach Wunsch eine Anmerkung ein und klicken Sie auf **Erzeugen**.
4. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass diese Änderung nicht rückgängig gemacht werden kann und dass alle nachfolgend erstellten Konfigurationspakete diese CCO enthalten müssen, damit Sie auf bereits installierten Endpoints wirksam werden können.
5. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass die Aktualisierung erfolgreich war und dass eine CCO erzeugt wurde, die in alle Konfigurationspakete aufgenommen werden soll. Klicken Sie auf **OK**.
6. Klicken Sie im **Extras** Menü auf **Konfigurationspakete**.

7. Wählen Sie **Pakete für Managed Clients**.
8. Klicken Sie auf **Konfigurationspaket hinzufügen** und geben Sie einen Namen Ihrer Wahl für das Konfigurationspaket ein.
9. Ordnen Sie einen **Primären Server** zu (der **Sekundäre Server** ist nicht notwendig).
10. Wählen Sie die zuvor zur Aktualisierung des Unternehmenszertifikats erstellte **CCO**.
11. Wählen Sie den Modus für die **Transportverschlüsselung**, der bestimmt, wie die Verbindung zwischen SafeGuard Enterprise Client und SafeGuard Enterprise Server verschlüsselt wird: SafeGuard-Transportverschlüsselung oder SSL-Verschlüsselung.

    Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung. SSL-Verschlüsselung wird standardmäßig ausgewählt. Weitere Informationen zur Absicherung von Transportverbindungen mit SSL finden Sie in der *SafeGuard Enterprise Installationsanleitung*.
12. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
13. Klicken Sie auf **Konfigurationspaket erstellen**.

    WennSie als Modus für die **Transportverschlüsselung** die SSL-Verschlüsselung ausgewählt haben, wird die Serververbindung validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Starten Sie alle SGN Server neu. Sie müssen das Paket auf den Endpoints verteilen und installieren.

13.2 Ersetzen des Unternehmenszertifikats

Das Ersetzen des Unternehmenszertifikats ist notwendig, wenn Sie einen Endpoint von einer Standalone-Umgebung in eine andere verschieben möchten. Der zu verschiebende Endpoint benötigt das Unternehmenszertifikat der Umgebung, in die er verschoben werden soll. Andernfalls akzeptiert der Endpoint keine Richtlinien in der neuen Umgebung. Die Vorgänge, die zum Ersetzen des Unternehmenszertifikats notwendig sind, können im sowohl im SafeGuard Management Center als auch im SafeGuard Policy Editor ausgeführt werden. In der folgenden Beschreibung wird für das SafeGuard Management Center und den SafeGuard Policy Editor der Begriff Management-Konsole verwendet, da der Vorgang des Ersetzens des Unternehmenszertifikats in beiden Fällen identisch ist.

Folgende Voraussetzungen müssen erfüllt sein:

Legen Sie die Ausgangs- und die Ziel Management Center/Policy Editor Umgebung fest. Die Ausgangs-Management-Konsole ist die, die Sie für das Erstellen der Konfigurationspakete für die Endpoints, die verschoben werden sollen, benutzt haben. Das Ziel ist die Management-Konsole, in die die Endpoints verschoben werden sollen.

So ersetzen Sie das Unternehmenszertifikat:

1. Exportieren Sie in der Ziel-Management-Konsole das Unternehmenszertifikat: Klicken Sie im Menü **Extras** auf **Optionen**. Wechseln Sie in die Registerkarte **Zertifikate** und klicken Sie im Bereich **Unternehmenszertifikat** auf **Exportieren**. Wenn aufgefordert, geben Sie ein Kennwort für den Zertifikatsspeicher ein und bestätigen Sie es und wählen Sie das Zielverzeichnis und den Dateinamen. Das Unternehmenszertifikat wird exportiert (cer-Datei).

2. Klicken Sie in der Ausgangs-Management-Konsole im **Extras** Menü auf **Optionen**. Wählen Sie die Registerkarte **Zertifikate** und klicken Sie im Bereich **Anforderung** auf **Erzeugen**. Wählen Sie im **CCO erzeugen** Dialog das Ziel-Unternehmenszertifikat aus, dass Sie in der Ziel-Management-Konsole exportiert haben (Schritt 1). Stellen Sie sicher, dass es sich um das gewünschte Zertifikat handelt. Klicken Sie auf **Erzeugen** und wählen Sie ein Zielverzeichnis und einen Dateinamen für die .cco-Datei aus. Bestätigen Sie, dass Sie eine **Company Certificate Change Order** erstellen möchten. Bitte beachten Sie, dass eine Company Certificate Change Order nicht an spezifische Endpoints gebunden ist. Mit einer Company Certificate Change Order lässt sich jeder Client der Ausgangsumgebung verschieben.
3. In der Ziel-Management-Konsole müssen Sie die in der Ausgangs-Management-Konsole erzeugte Company Certificate Change Order importieren. Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** und wählen Sie dann die Registerkarte **CCOs**. Klicken Sie auf **Importieren**.
4. Wählen Sie im Dialog **CCO importieren** die in der Ausgangs-Management-Konsole erzeugte Company Certificate Change Order und geben Sie einen Namen und nach Wunsch eine Beschreibung für die Company Certificate Change Order ein. Klicken Sie auf **OK**.
5. Erstellen Sie in der Ziel-Management-Konsole ein Konfigurationspaket: Klicken Sie im **Extras** Menü auf **Konfigurationspakete...** > **Pakete für Standalone Clients** und fügen Sie ein neues Konfigurationspaket hinzu. Wählen Sie die importierte Company Certificate Change Order aus dem Dropdown-Menü der Spalte **CCO**. Geben Sie unter **Konfigurationspaket-Ausgabepfad** einen Speicherort an. Klicken Sie auf **Konfigurationspaket erstellen**. Das Konfigurationspaket wird am angegebenen Speicherort angelegt.
6. Installieren Sie dieses Konfigurationspaket auf allen Endpoints, die Sie von der Ausgangs- in die Zielumgebung verschieben möchten.

13.3 Verwalten von Company Certificate Change Orders

Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**. Alle erzeugten CCOs werden in der Registerkarte **CCOs** angezeigt.

Im unteren Bereich des Dialogs werden detaillierte Informationen zur ausgewählten CCO angezeigt.

Wenn die CCO für die Erneuerung des Unternehmenszertifikats erstellt wurde, wird das **Quell-Unternehmenszertifikat** aktualisiert. Wenn die CCO für eine Verschiebung von Endpoints erstellt wurde, erneuern Sie das Unternehmenszertifikat der Umgebung, deren Endpoints in eine andere Umgebung verschoben werden sollen.

Das **Ziel-Unternehmenszertifikat** ist das neue Unternehmenszertifikat, wenn die CCO zur Aktualisierung des Unternehmenszertifikats oder des Unternehmenszertifikats der Umgebung, in die die Endpoints verschoben werden sollen, erzeugt wurde.

Unter den Zertifikatsinformationen wird angegeben, für welche Vorgänge die ausgewählte CCO verwendet werden kann.

Hinweis: Für die Verwaltung von CCOs benötigen Sie das Recht **CCOs verwalten**.

13.3.1 Import

Um beim Erstellen von Konfigurationspaketen die von einem anderen Management-Werkzeug erstellte CCO auszuwählen um das Unternehmenszertifikat zu ändern, müssen Sie es erst importieren.

Klicken Sie auf **Importieren...**, um einen Dialog zu öffnen, in dem Sie die CCO auswählen und benennen können. Der hier eingegebene Name wird in der Registerkarte **CCOs** unter **Konfigurationspakete** angezeigt.

13.3.2 Export

Mit der **Exportieren** Funktion lassen sich in der Datenbank gespeicherte CCOs als .cco-Dateien exportieren.

14 Mit Richtlinien arbeiten

Die folgenden Abschnitte beschreiben richtlinienrelevanten Vorgänge, z. B. das Erstellen, Gruppieren und Sichern von Richtlinien.

Hinweis: Für das Zuweisen, Entfernen oder Bearbeiten von Richtlinien benötigen Sie das Zugriffsrecht **Voller Zugriff** für die relevanten Objekte sowie für jede Gruppe, die für die jeweiligen Richtlinien aktiviert ist.

Eine Beschreibung aller verfügbaren SafeGuard Enterprise-Richtlinieneinstellungen finden Sie unter Richtlinieneinstellungen (Seite 126).

14.1 Anlegen von Richtlinien

1. Melden Sie sich mit dem Kennwort, das Sie während der Erstkonfiguration festgelegt haben, am SafeGuard Management Center an.
2. Klicken Sie im Navigationsbereich auf **Richtlinien**.
3. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien** und wählen Sie im Kontextmenü den Befehl **Neu**.
4. Wählen Sie den Richtlinientyp aus.

   Es wird ein Dialog für die Benennung der neuen Richtlinie angezeigt.

5. Geben Sie einen Namen und optional eine Beschreibung für die neue Richtlinie ein.

   Richtlinien für den Geräteschutz:

   Wenn Sie eine Richtlinie dieses Typs erstellen, müssen Sie auch ein Ziel für den Geräteschutz angeben. Mögliche Ziele sind:

   - Massenspeicher (Boot-Laufwerke/Andere Volumes)
   - Wechselmedien
   - Optische Laufwerke
   - Datenträgermodelle
   - Einzelne Datenträger
   - Cloud Storage

   Für jedes Ziel muss eine eigene Richtlinie angelegt werden. Sie können die einzelnen Richtlinien später z. B. zu einer Richtliniengruppe mit der Bezeichnung *Verschlüsselung* zusammenfassen.

6. Klicken Sie auf **OK**.

Die neu angelegte Richtlinie wird im Navigationsfenster unter **Richtlinien** angezeigt. Im Aktionsbereich werden alle Einstellungen für den gewählten Richtlinientyp angezeigt. Die Einstellungen können dort geändert werden.

14.2 Bearbeiten von Richtlinieneinstellungen

Wenn Sie im Navigationsfenster eine Richtlinie auswählen, können Sie deren Einstellungen im Aktionsbereich bearbeiten.

Hinweis:

	Das rote Symbol vor dem Text **nicht konfiguriert** gibt an, dass für diese Einstellung ein Wert festgelegt werden muss. Sie können die Richtlinie erst speichern, wenn Sie eine andere Einstellung als **nicht konfiguriert** ausgewählt haben.

Setzen von Einstellungen auf Standardwerte

In der Symbolleiste stehen folgende Symbole für Richtlinieneinstellungen zur Verfügung:

Symbol	Richtlinieneinstellung
	Zeigt Standardwerte für Richtlinieneinstellungen an, die nicht konfiguriert wurden (Einstellung **nicht konfiguriert**). Die Standardwerte für Richtlinieneinstellungen werden standardmäßig angezeigt. Klicken Sie auf das Symbol, um die Standardwerte auszublenden.
	Setzt die markierte Richtlinieneinstellung auf **nicht konfiguriert**.
	Setzt alle Richtlinieneinstellungen eines Bereichs auf **nicht konfiguriert**.
	Setzt den Standardwert für die markierte Richtlinieneinstellung.
	Setzt alle Richtlinieneinstellungen eines Bereichs auf den Standardwert.

Unterscheidung zwischen maschinen- und benutzerspezifischen Richtlinien

Richtlinienfarbe blau	Richtlinie wird nur für Maschinen angewandt, nicht für Benutzer.
Richtlinienfarbe schwarz	Richtlinie wird für Maschinen und Benutzer angewandt.

14.3 Richtliniengruppen

SafeGuard Enterprise Richtlinien können in Richtliniengruppen zusammengefasst werden. Eine Richtliniengruppe kann verschiedene Richtlinientypen enthalten. Im SafeGuard Management Center steht eine **Default** Richtliniengruppe zur Verfügung, die standardmäßig unter **Benutzer und Computer** zu **Stamm** zugewiesen wird.

Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten.

Eine definierte Richtlinieneinstellung überschreibt Einstellungen aus anderen Richtlinien, wenn

- die Richtlinie mit dieser Einstellung eine höhere Priorität hat.
- die Richtlinieneinstellung noch nicht definiert ist (**nicht konfiguriert**).

Hinweis: Überlappende Richtlinien, die einer Gruppe zugeordnet sind, können zu einer falschen Ermittlung der Prioritäten führen. Verwenden Sie separate Richtlinieneinstellungen.

Ausnahme Geräteschutz:

Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volume) angelegt werden. Weisen sie auf verschiedene Ziele, werden sie addiert.

14.3.1 Zusammenfassen von Richtlinien zu Gruppen

Voraussetzung: Die einzelnen Richtlinien der verschiedenen Typen müssen angelegt sein.

1. Klicken Sie im Navigationsbereich auf **Richtlinien**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien-Gruppen** und wählen Sie **Neu**.
3. Klicken Sie auf **Neue Richtlinien-Gruppe**. Es wird ein Dialog für die Benennung der Richtlinien-Gruppe angezeigt.
4. Geben Sie einen eindeutigen Namen und optional eine Beschreibung für die Richtlinien-Gruppe ein. Klicken Sie auf **OK**.
5. Die neu angelegte Richtlinie-Gruppe wird im Navigationsfenster unter **Richtlinien-Gruppen** angezeigt.
6. Wählen Sie die Richtlinien-Gruppe aus. Im Aktionsbereich werden alle für das Gruppieren der Richtlinien notwendigen Elemente angezeigt.
7. Zum Gruppieren der Richtlinien ziehen Sie sie aus der Liste der verfügbaren Richtlinien in den Richtlinienbereich.

8. Sie können für jede Richtlinie eine **Priorität** festlegen, indem Sie die Richtlinie über das Kontextmenü nach oben oder unten reihen.

   Wenn Sie Richtlinien vom selben Typ in einer Gruppe zusammenfassen, werden die Einstellungen automatisch vereinigt. Sie können dafür eine Auswertungsreihenfolge festlegen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Ist eine Einstellung auf **nicht konfiguriert** gesetzt, wird die Einstellung in einer niedriger priorisierten Richtlinie **nicht überschrieben**.

   Ausnahme Geräteschutz:

   Richtlinien für den Geräteschutz werden nur vereinigt, wenn sie für dasselbe Ziel (z. B. Boot-Volume) angelegt werden. Weisen sie auf verschiedene Ziele, werden sie addiert.

9. Speichern Sie die Richtliniengruppe über **Datei > Speichern**.

Die Richtliniengruppe enthält nun die Einstellungen aller einzelnen Richtlinien.

14.3.2 Ergebnis der Gruppierung

Das Ergebnis der Zusammenfassung wird in einer eigenen Ansicht dargestellt.

Klicken Sie zum Anzeigen der Zusammenfassung auf die Registerkarte **Ergebnis**.

- Für jeden Richtlinien-Typ steht eine eigene Registerkarte zur Verfügung.

  Die aus der Zusammenfassung der einzelnen Richtlinien resultierenden Einstellungen werden angezeigt.

- Für Richtlinien zum Geräteschutz werden Registerkarten für jedes Ziel der Richtlinie angezeigt (z. B. Boot-Volumes, Laufwerk X: usw.).

14.4 Erstellen von Sicherungskopien von Richtlinien und Richtliniengruppen

Sie können Sicherungskopien von Richtlinien und Richtliniengruppen in Form von XML-Dateien erstellen. Falls notwendig, lassen sich die betreffenden Richtlinien/Richtliniengruppen daraufhin aus diesen XML-Dateien wiederherstellen.

1. Wählen Sie die Richtlinie/Richtliniengruppe im Navigationsfenster unter **Richtlinien** bzw. **Richtlinien-Gruppen** aus.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie sichern**.

   Hinweis: Der Befehl **Richtlinie sichern** steht auch im Menü **Aktionen** zur Verfügung.

3. Geben Sie im Dialog **Speichern unter** einen Dateinamen für die XML-Datei an und wählen Sie das Verzeichnis, in dem die Datei gespeichert werden soll. Klicken Sie auf **Speichern**.

Die Sicherungskopie der Richtlinie/Richtliniengruppe ist im angegebenen Verzeichnis als XML-Datei abgelegt.

14.5 Wiederherstellen von Richtlinien und Richtliniengruppen

So stellen Sie eine Richtlinie/Richtliniengruppe aus einer XML-Datei wieder her:

1. Klicken Sie im Navigationsfenster auf **Richtlinien/Richtliniengruppen**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie im angezeigten Kontextmenü **Richtlinie wiederherstellen**.

   Hinweis: Der Befehl **Richtlinie wiederherstellen** steht auch im Menü **Aktionen** zur Verfügung.

3. Wählen Sie die XML-Datei für die Wiederherstellung der Richtlinie/Richtliniengruppe aus und klicken Sie auf **Öffnen**.

Die Richtlinie/Richtliniengruppe ist wiederhergestellt.

14.6 Zuweisen von Richtlinien

Um Richtlinien zuzuweisen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für alle beteiligten Objekte.

1. Klicken Sie auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsbereich das gewünschte Objekt aus (z. B. Benutzer, Gruppe oder Container).
3. Wechseln Sie in die Registerkarte **Richtlinien**.

   Im Aktionsbereich werden alle für die Zuweisung der Richtlinie notwendigen Elemente angezeigt.

4. Zum Zuweisen einer Richtlinie ziehen Sie sie aus der Liste der verfügbaren Richtlinien in die Registerkarte **Richtlinien**.
5. Sie können für jede Richtlinie eine **Priorität** festlegen, indem Sie die Richtlinie über das Kontextmenü nach oben oder unten reihen. Die Einstellungen einer höher gereihten Richtlinie überschreiben jene einer niedriger priorisierten. Wenn Sie für eine Richtlinie **Kein Überschreiben** aktivieren, können die Einstellungen dieser Richtlinie nicht von anderen überschrieben werden.

   Hinweis: Wenn Sie bei einer Richtlinie mit niedrigerer Priorität die Option **Kein Überschreiben** aktivieren, so zieht diese Richtlinie, trotz niedrigerer Priorität gegenüber einer Richtlinie mit einer höheren Priorität.

   Um die Einstellungen **Priorität** oder **Kein Überschreiben** für Richtlinien im Bereich **Benutzer & Computer** zu ändern, benötigen Sie das Zugriffsrecht **Voller Zugriff** für alle Objekte, denen die Richtlinien zugewiesen sind. Wenn Sie das Zugriffsrecht **Voller Zugriff** nicht für alle Objekte haben, können die Einstellungen nicht bearbeitet werden. Wenn Sie versuchen, die Felder zu bearbeiten, wird eine Info-Meldung angezeigt.

6. Im Aktivierungsbereich werden die Gruppen .Authentisierte Benutzer - bzw. Computer angezeigt.

Die Richtlinie gilt für alle Gruppen innerhalb der OU bzw. Domäne.

14.6.1 Aktivieren von Richtlinien für einzelne Gruppen

Richtlinien werden immer einer OU bzw. einer Domäne oder Arbeitsgruppe zugewiesen. Sie gelten standardmäßig für alle Gruppen in diesen Container-Objekten (die Gruppen .Authentisierte Benutzer und .Authentisierte Computer werden im Aktivierungsbereich angezeigt).

Sie können aber auch Richtlinien festlegen und sie für eine einzelne oder mehrere Gruppen aktivieren. Diese Richtlinien gelten dann ausschließlich für diese Gruppen.

Hinweis: Um Richtlinien für einzelne Gruppen zu aktivieren, benötigen Sie das Zugriffsrecht **Voller Zugriff** für die relevante Gruppe.

1. Weisen Sie die Richtlinie der OU, in der sich die Gruppe befindet, zu.
2. Im Aktivierungsbereich werden die Gruppen .Authentisierte Benutzer und .Authentisierte Computer angezeigt.
3. Ziehen Sie diese beiden Gruppen aus dem Aktivierungsbereich in die Liste der **Verfügbaren Gruppen**. Die Richtlinie ist in dieser Konstellation für keinen Benutzer und keinen Computer wirksam.
4. Ziehen Sie jetzt die gewünschte Gruppe (oder auch mehrere Gruppen) aus der Liste der **Verfügbaren Gruppen** in den Aktivierungsbereich.

Diese Richtlinie gilt jetzt ausschließlich für diese Gruppe.

Wurden der übergeordneten OU ebenfalls Richtlinien zugeordnet, gilt diese Richtlinie für diese Gruppe zusätzlich zu jenen, die für die gesamte OU festgelegt wurden.

14.7 Verwalten von Richtlinien unter Benutzer & Computer

Neben dem Bereich **Richtlinien** im SafeGuard Management Center können Sie den Inhalt einer Richtlinie auch dort einsehen und ändern, wo die Richtlinienzuweisung erfolgt: unter **Benutzer & Computer**.

1. Klicken Sie auf **Benutzer & Computer**.
2. Wählen Sie im Navigationsbereich das gewünschte Containerobjekt.
3. Sie können Richtlinien von zwei Orten aus öffnen, um sie einzusehen oder zu ändern.
   - Wechseln Sie in die Registerkarte **Richtlinien**, oder
   - wechseln Sie in die Registerkarte **RSOP**.
4. Klicken Sie mit der rechten Maustaste auf die gewünschte zugewiesene oder verfügbare Richtlinie und wählen Sie **Öffnen** aus dem Kontextmenü.

   Der Richtliniendialog wird angezeigt und Sie können die Richtlinieneinstellungen einsehen und bearbeiten.
5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
6. Um die Richtlinieneigenschaften aufzurufen, klicken Sie mit der rechten Maustaste auf die gewünschte Richtlinie und wählen Sie **Eigenschaften** aus dem Kontextmenü.

   Der **Eigenschaften** Dialog für die Richtlinie wird angezeigt. Hier können Sie unter **Allgemein** und **Zuweisung** die entsprechenden Informationen einsehen.

14.8 Deaktivieren der Übertragung von Richtlinien

Als Sicherheitsbeauftragter können Sie die Übertragung von Richtlinien an Endpoints deaktivieren. Klicken Sie hierzu in der SafeGuard Management Center Symbolleiste auf die Schaltfläche **Richtlinienverteilung aktivieren/deaktivieren** oder wählen Sie im Menü **Bearbeiten** den Befehl **Richtlinienverteilung aktivieren/deaktivieren**. Nach der Deaktivierung der Richtlinienübertragung werden keine Richtlinien mehr an die Endpoints geschickt. Um die Deaktivierung der Richtlinienverteilung rückgängig zu machen, klicken Sie noch einmal auf die Schaltfläche oder wählen Sie noch einmal den Menübefehl.

Hinweis: Um die Übertragung von Richtlinien zu deaktivieren, benötigen Sie als Sicherheitsbeauftragter die Berechtigung „Richtlinienverteilung aktivieren/deaktivieren". Den beiden vordefinierten Rollen Haupt-Sicherheitsbeauftragter und Sicherheitsbeauftragter ist diese Berechtigung standardmäßig zugewiesen. Neu angelegten benutzerdefinierten Rollen kann diese Berechtigung jederzeit zugewiesen werden.

14.9 Regeln für die Zuweisung und Auswertung von Richtlinien

Die Verwaltung und Auswertung von Richtlinien folgt den in diesem Abschnitt dargestellten Regeln.

14.9.1 Zuweisen und Aktivieren von Richtlinien

Damit eine Richtlinie für einen Benutzer/Computer wirksam werden kann, muss sie einem Container-Objekt (Root-Knoten, Domäne, OU, BuiltIn-Container oder Arbeitsgruppe) zugewiesen werden. Damit die zugewiesene Richtlinie für Benutzer/Computer wirksam wird, werden beim Zuweisen einer Richtlinie an einer beliebigen Stelle in der Hierarchie alle Computer (authentisierte Computer) und alle Benutzer (authentisierte Benutzer) automatisch aktiviert (die alleinige Zuweisung ohne Aktivierung reicht nicht aus). In diesen Gruppen sind alle Benutzer bzw. Computer zusammengefasst.

14.9.2 Vererbung von Richtlinien

Vererbung von Richtlinien ist nur zwischen Container-Objekten möglich. Innerhalb eines Containers - vorausgesetzt er enthält keine weiteren Container-Objekte - können Richtlinien nur aktiviert werden (auf Gruppenebene). Vererbung zwischen Gruppen ist nicht möglich.

14.9.3 Vererbungsreihenfolge von Richtlinien

Werden Richtlinien entlang einer Hierarchiekette zugewiesen, so wirkt jene Richtlinie am stärksten, die näher beim Zielobjekt (Benutzer/Computer) ist. Das bedeutet: mit der Entfernung zum Zielobjekt verliert die Richtlinie immer mehr an Kraft - wenn nähere Richtlinien vorhanden sind.

14.9.4 Direkte Zuweisung von Richtlinien

Der Benutzer/Computer erhält eine Richtlinie, die direkt dem Container-Objekt, in dem er sich tatsächlich befindet (Mitgliedschaft als Benutzer einer Gruppe, die sich in einem anderen

Container-Objekt befindet, alleine reicht nicht aus), zugewiesen wurde. Das Container-Objekt hat diese Richtlinie nicht geerbt!

14.9.5 Indirekte Zuweisung von Richtlinien

Der Benutzer/Computer erhält eine Richtlinie, die das Container-Objekt, in dem er sich tatsächlich befindet (die Mitgliedschaft in einer Gruppe, die sich in einem anderen Container-Objekt befindet, als der Benutzer, reicht nicht aus), von einem ihr übergeordneten Container-Objekt geerbt hat.

14.9.6 Aktivieren/Deaktivieren von Richtlinien

Damit eine Richtlinie für einen Computer/Benutzer wirken kann, muss diese auf Gruppenebene aktiviert werden (Richtlinien können ausschließlich auf Gruppenebene aktiviert werden). Es spielt keine Rolle, ob sich diese Gruppe im selben Container-Objekt befindet, oder nicht. Wichtig ist hier nur, dass der Benutzer oder Computer eine direkte bzw. indirekte (durch Vererbung) Zuordnung der Richtlinie erhalten hat.

Befindet sich ein Computer oder Benutzer außerhalb einer OU oder Vererbungslinie und ist Mitglied einer Gruppe, die sich innerhalb dieser OU befindet, so gilt diese Aktivierung für diesen Benutzer oder Computer **nicht**. Denn für diesen Benutzer oder Computer ist keine gültige Zuweisung (direkt bzw. indirekt) vorhanden. Die Gruppe wurde zwar aktiviert, aber eine Aktivierung kann nur für Benutzer und Computer gelten, für die auch eine Richtlinienzuweisung besteht. Das heißt, die Aktivierung von Richtlinien kann nicht über Container- Grenzen hinausgehen, wenn keine direkte oder indirekte Richtlinienzuweisung für dieses Objekt existiert.

Eine Richtlinie wird wirksam, wenn sie entweder bei Benutzergruppen oder Computergruppen aktiviert wurde. Es werden die Benutzergruppen und dann die Computergruppen ausgewertet (auch authentisierte Benutzer und authentisierte Computer sind Gruppen). Beide Ergebnisse werden ODER-verknüpft. Liefert diese ODER-Verknüpfung einen positiven Wert für die Computer/Benutzer-Beziehung, gilt die Richtlinie.

Hinweis: Werden mehrere Richtlinien für ein Objekt aktiv, werden die einzelnen Richtlinien unter Einhaltung der beschriebenen Regeln, vereinigt. Das heißt, die tatsächlichen Einstellungen für ein Objekt können aus mehreren unterschiedlichen Richtlinien zusammengesetzt werden.

Für eine Gruppe gibt es folgende Aktivierungseinstellungen:

- Aktiviert

  Eine Richtlinie wurde zugewiesen. Die Gruppe wird im Aktivierungsbereich des SafeGuard Management Centers angezeigt.

- Nicht aktiviert

  Eine Richtlinie wurde zugewiesen. Die Gruppe befindet sich nicht im Aktivierungsbereich.

Wird eine Richtlinie einem Container zugewiesen, dann bestimmt die Aktivierungseinstellung für eine Gruppe (aktiviert), ob diese Richtlinie an diesem Container in die Berechnung der resultierenden Richtlinie einfließt.

Vererbte Richtlinien können durch diese Aktivierungen nicht kontrolliert werden. Hierfür müsste an der lokaleren OU **Richtlinienvererbung blockieren** gesetzt werden, damit die globalere Richtlinie hier nicht wirken kann.

14.9.7 Benutzer-/Gruppeneinstellungen

Richtlinieneinstellungen für Benutzer (im SafeGuard Management Center **schwarz** dargestellt), ziehen stärker, als Richtlinieneinstellungen für Computer (im SafeGuard Management Center **blau** dargestellt). Werden bei einer Richtlinie für Computer Benutzereinstellungen festgelegt, werden diese Einstellungen durch die Richtlinie für den Benutzer überschrieben.

Hinweis: Nur die Benutzereinstellungen werden überschrieben. Sollte eine Richtlinie für Benutzer auch Maschineneinstellungen beinhalten (**blau** dargestellte Einstellungen) werden diese nicht von einer Benutzerrichtlinie überschrieben!

Beispiel 1:

Wird für eine Computergruppe die Kennwortlänge 4 definiert, die Benutzergruppe hat aber für dieselbe Einstellung den Wert 3, gilt für diesen Benutzer auf einem Computer der Computergruppe, ein Kennwort mit der Länge 3.

Beispiel 2:

Wird für eine Benutzergruppe ein Serverintervall von 1 Minute definiert und für eine Computergruppe der Wert 3, so wird der Wert 3 verwendet, da es sich beim Wert 1 Minute um eine Maschineneinstellung, die in einer Richtlinie für Benutzer definiert wurde, handelt.

14.9.8 Sich widersprechende Verschlüsselungsrichtlinien

Es werden zwei Richtlinien - P1 und P2 - angelegt. Für P1 wurde eine dateibasierende Verschlüsselung für Laufwerk E:\ definiert und für P2 eine volume-basierende Verschlüsselung für Laufwerk E:\. P1 wird der OU **FBE-User** und P2 der OU **VBE-User** zugewiesen.

Fall 1: Ein Benutzer aus OU **FBE-User** meldet sich zuerst am Client W7-100 (Container Computer) an. Laufwerk E:\ ist dateibasierend verschlüsselt. Meldet sich ein Benutzer danach aus der OU **VBE-User** am Client W7-100 an, so wird das Laufwerk E:\ volume-basierend verschlüsselt. Haben beide Benutzer dieselben Schlüssel, können beide auf die Laufwerke bzw. Dateien zugreifen.

Fall 2: Ein Benutzer aus der OU **VBE-User** meldet sich zuerst am Computer W7-100 (Container Computer) an. Das Laufwerk ist mit volume-basierender Verschlüsselung verschlüsselt. Meldet sich nun ein Benutzer der OU **FBE-User** an und hat dieser einen gemeinsamen Schlüssel mit den Benutzern aus der OU **VBE-User**, so wird das Laufwerk E:\ (die volume-basierende Verschlüsselung bleibt erhalten) innerhalb der volume-basierenden Verschlüsselung dateibasierend verschlüsselt. Hat der Benutzer aus der OU **FBE-User** allerdings keinen gemeinsamen Schlüssel, kann er auf das Laufwerk E:\ nicht zugreifen.

14.9.9 Priorisierung innerhalb einer Zuweisung

Innerhalb einer Zuweisung, hat die Richtlinie mit der höchsten Priorität (1) Vorrang gegenüber einer Richtlinie mit einer geringeren Priorität.

Hinweis: Wurde auf gleicher Ebene eine Richtlinie mit niedriger Priorität, aber mit der Option **Kein Überschreiben**, zugeordnet, so zieht die Richtlinie trotz niedrigerer Priorität gegenüber den Richtlinien mit der höheren Priorität.

14.9.10 Priorisierung innerhalb einer Gruppe

Innerhalb einer Gruppe, hat die Richtlinie mit der höchsten Priorität (1) Vorrang gegenüber einer Richtlinie mit einer geringeren Priorität.

14.9.11 Statusindikatoren

Durch das Setzen von Statusindikatoren kann das Standardregelwerk der Richtlinien verändert werden.

- **Richtlinienvererbung blockieren**

  Wird direkt bei dem Container gesetzt, der keine übergeordneten Richtlinien empfangen will (Rechtsklick auf das Objekt im Navigationsfenster > Eigenschaften).

  Soll ein Container-Objekt keine Richtlinie eines übergeordneten Objektes erben, können Sie das durch das Setzen von **Richtlinienvererbung blockieren** verhindern. Ist **Richtlinienvererbung blockieren** gesetzt, werden keine übergeordneten Richtlinieneinstellungen für dieses Container-Objekt wirksam (Ausnahme: **Kein Überschreiben** wurde bei der Richtlinienzuweisung aktiviert).

- **Kein Überschreiben**

  Wird bei der Zuweisung gesetzt und bedeutet, dass diese Richtlinie nicht von anderen überschrieben werden kann.

  Je weiter die Richtlinienzuweisung mit **Kein Überschreiben** vom Zielobjekt entfernt ist, umso stärker wird die Wirkung dieser Richtlinie für alle untergeordneten Container-Objekte. Das heißt: **Kein Überschreiben** eines übergeordneten Containers überschreibt die Richtlinieneinstellungen eines untergeordneten Containers. So kann z.B. eine Domänenrichtlinie definiert werden, deren Einstellungen nicht überschrieben werden können, auch nicht, wenn für eine OU **Richtlinienvererbung blockieren** gesetzt wurde!

  Hinweis: Wurde auf gleicher Ebene eine Richtlinie mit niedriger Priorität, aber mit der Option **Kein Überschreiben**, zugeordnet, so zieht die Richtlinie trotz niedrigerer Priorität gegenüber den Richtlinien mit der höheren Priorität.

14.9.12 Einstellungen in Richtlinien

14.9.12.1 Computereinstellungen wiederholen

Sie finden diese Einstellung unter:

Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen > Laden der Einstellungen > Richtlinien-Loopback**.

Wird bei einer Richtlinie vom Typ **Allgemeine Einstellungen** bei der Option **Richtlinien-Loopback** die Einstellung **Computereinstellungen wiederholen** ausgewählt und die Richtlinie „kommt“ von einem Computer (**Computereinstellungen wiederholen** hat für eine Benutzerrichtlinie keine Auswirkung), wird diese Richtlinie am Ende der Auswertung noch einmal ausgeführt. Dadurch werden etwaige Benutzereinstellungen wieder überschrieben und es gelten die Computereinstellungen. Für das neuerliche Schreiben werden sämtliche Computereinstellungen, die der Computer direkt oder indirekt bekommt (auch von Richtlinien die beim Richtlinien-Loopback **Computereinstellungen wiederholen** nicht gesetzt wurden), neu geschrieben.

14.9.12.2 Benutzer ignorieren

Sie finden diese Einstellung unter:

Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen > Laden der Einstellungen > Richtlinien-Loopback**.

Wird bei einer Richtlinie vom Typ **Allgemeine Einstellungen** für einen Computer bei der Option **Richtlinien-Loopback** die Einstellung **Benutzer ignorieren** ausgewählt und die Richtlinie „kommt“ von einer Maschine, werden nur die Maschineneinstellungen ausgewertet. Benutzereinstellungen werden nicht ausgewertet.

14.9.12.3 Kein Loopback

Sie finden diese Einstellung unter:

Richtlinien > Richtlinie vom Typ **Allgemeine Einstellungen > Laden der Einstellungen > Richtlinien-Loopback**.

Kein Loopback beschreibt das Standardverhalten. Benutzerrichtlinien gelten vor Computerrichtlinien.

14.9.12.4 Auswertung der Einstellungen „Benutzer ignorieren“ und „Computereinstellungen wiederholen“

Existieren aktive Richtlinienzuweisungen, werden zuerst die Maschinenrichtlinien ausgewertet und vereinigt. Ergibt diese Vereinigung der einzelnen Richtlinien bei der Option **Richtlinien-Loopback** den Wert **Benutzer ignorieren**, werden die Richtlinien, die für den Benutzer bestimmt gewesen wären, nicht mehr ausgewertet. Das bedeutet sowohl für den Benutzer, als auch für den Computer gelten die gleichen Richtlinien.

Gilt nach der Vereinigung der einzelnen Maschinenrichtlinien bei **Richtlinien-Loopback** der Wert **Computereinstellungen wiederholen**, werden die Benutzerrichtlinien mit den Maschinenrichtlinien vereinigt. Nach der Vereinigung, werden die Maschinenrichtlinien nochmals geschrieben und überschreiben gegebenenfalls Einstellungen aus den Benutzerrichtlinien. Ist eine Einstellung in beiden Richtlinien vorhanden, so ersetzt der Wert der Maschinenrichtlinie den Wert der Benutzerrichtlinie.

Ergibt die Vereinigung der einzelnen Maschinenrichtlinien den Standardwert (**Kein Richtlinien-Loopback**), so gilt: Benutzereinstellungen vor Maschineneinstellungen.

14.9.12.5 Ausführungsreihenfolge der Richtlinien

Benutzer ignorieren Computer

Computereinstellungen wiederholen Computer -> Benutzer -> Computer. Die erste „Maschinen-Ausführung“ wird für die Richtlinien benötigt, die schon vor der Benutzeranmeldung (z. B. Hintergrundbild bei der Anmeldung) geschrieben werden.

Kein Richtlinien-Loopback (Standardeinstellung): Computer -> Benutzer

14.9.13 Sonstige Definitionen

Die Entscheidung, ob es sich um eine Benutzer- bzw. Maschinenrichtlinie handelt, hängt von der Herkunft der Richtlinie ab. Ein Benutzerobjekt „bringt“ eine Benutzerrichtlinie mit, ein Computer „bringt“ eine Computerrichtlinie mit. Dieselbe Richtlinie kann bei unterschiedlicher Sicht, sowohl Computer- als auch Benutzerrichtlinie sein.

- **Benutzerrichtlinie**

  Jene Richtlinie, die der Benutzer zur Auswertung bereitstellt. Wenn eine Richtlinie nur über einen Benutzer kommt, dann werden die maschinenbezogenen Einstellungen dieser Richtlinie nicht verwendet. Das heißt, es gelten keine computerbezogenen Einstellungen. Es gelten die Standardwerte.

- **Computerrichtlinie**

  Jene Richtlinie, die die Maschine zur Auswertung bereitstellt. Wenn eine Richtlinie nur über einen Computer kommt, dann werden auch die benutzerspezifischen Einstellungen dieser Richtlinie verwendet! Die Computerrichtlinie stellt dann eine „für alle Benutzer" Richtlinie dar.

15 Mit Konfigurationspaketen arbeiten

Im SafeGuard Management Center lassen sich Konfigurationspakete der folgenden Typen erstellen:

- **Konfigurationspaket für zentral verwaltete Endpoints**

  Endpoints, die eine Verbindung zum SafeGuard Enterprise Server haben, erhalten Ihre Richtlinien über den Server. Für den erfolgreichen Einsatz der SafeGuard Enterprise Client Software nach der Installation müssen Sie zunächst ein Konfigurationspaket für zentral verwaltete Computer erzeugen und es auf den Computern installieren.

  Nach der ersten Konfiguration der Endpoints über das Konfigurationspaket erhalten die Endpoints Richtlinien über den SafeGuard Enterprise Server, wenn Sie diese im Bereich **Benutzer & Computer** des SafeGuard Management Center zugewiesen haben.

- **Konfigurationspaket für Standalone-Endpoints**

  Standalone-Endpoints haben niemals eine Verbindung zum SafeGuard Enterprise Server, sie laufen im Standalone-Modus. Die Computer erhalten ihre Richtlinien über Konfigurationspakete. Für den erfolgreichen Einsatz der Software müssen Sie ein Konfigurationspaket mit den relevanten Richtliniengruppen erstellen und es über unternehmenseigene Verteilungsmechanismen an die Endpoints verteilen. Wenn Sie Richtlinieneinstellungen ändern, müssen Sie jeweils neue Konfigurationspakete erstellen und an die Endpoints verteilen.

  Hinweis: Konfigurationspakete für Standalone-Endpoints können nur auf Windows Endpoints verwendet werden.

- **Konfigurationspaket für den SafeGuard Enterprise Server**

  Für den erfolgreichen Einsatz der Software müssen Sie ein Konfigurationspaket für den SafeGuard Enterprise Server erstellen, das die Datenbank sowie die SSL-Verbindung definiert, Scripting API aktiviert, usw.

- **Konfigurationspaket für Macs**

  Über dieses Konfigurationspaket erhalten Macs die Server-Adresse und das Unternehmenszertifikat. Die Macs übermitteln ihre Statusinformationen, die dann im SafeGuard Management Center angezeigt werden. Informationen zum Erstellen von Konfigurationspaketen für Macs finden Sie unter Erstellen von Konfigurationspaketen für Macs (Seite 293).

Hinweis: Überprüfen Sie Ihr Netzwerk und Ihre Computer in regelmäßigen Abständen auf veraltete oder nicht benutzte Konfigurationspakete und löschen Sie diese aus Sicherheitsgründen. Deinstallieren Sie vor der Installation eines neuen Konfigurationspakets auf dem Computer/Server jeweils die veralteten Konfigurationspakete.

15.1 Erzeugen eines Konfigurationspakets für zentral verwaltete Endpoints

Voraussetzungen

- Prüfen Sie im **Benutzer & Computer** Navigationsbereich in der Registerkarte **Bestand**, ob für die Endpoints, die das neue Konfigurationspaket erhalten sollen, ein Wechsel des Unternehmenszertifikats erforderlich ist. Wenn das Feld **Aktuelles Unternehmenszertifikat** nicht aktiviert ist, unterscheiden sich das derzeit aktive Unternehmenszertifikat in der SafeGuard Enterprise Datenbank und auf dem Computer voneinander. Daher ist ein Wechsel des Unternehmenszertifikats erforderlich.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Managed Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht notwendig).
6. Falls erforderlich, geben Sie eine Richtliniengruppe an, die auf die Endpoints angewendet werden soll. Diese müssen Sie zuvor im SafeGuard Management Center erstellt haben. Wenn Sie für Aufgaben nach der Installation auf dem Endpoint Service Accounts verwenden möchten, stellen Sie sicher, dass die entsprechende Richtlinieneinstellung in dieser ersten Richtliniengruppe definiert ist (siehe Service Account-Listen für die Windows-Anmeldung (Seite 115)).
7. Wenn sich das derzeit aktive Unternehmenszertifikat in der SafeGuard Enterprise Datenbank von dem auf den Endpoints, die das neue Konfigurationspaket erhalten sollen, unterscheidet, wählen Sie die relevante **CCO** (Company Certificate Change Order). Ist das Feld **Aktuelles Unternehmenszertifikat** in der Registerkarte **Bestand** der relevanten Domäne, der OU oder des Computers unter **Benutzer & Computer** nicht aktiviert, so ist ein Wechsel des Unternehmenszertifikats erforderlich. Informationen zur erforderlichen CCO (Company Certificate Change Order) finden Sie in der Registerkarte **CCOs** der Funktion **Konfigurationspakete** im Menü **Extras**.

   Hinweis: Die Installation des neuen Konfigurationspakets schlägt fehl, wenn die derzeit aktiven Unternehmenszertifikate in der SafeGuard Enterprise Datenbank und auf dem Endpoint nicht übereinstimmen und keine passende **CCO** im Paket enthalten ist.

8. Wählen Sie den Modus für die **Transportverschlüsselung**, der bestimmt, wie die Verbindung zwischen SafeGuard Enterprise Client und SafeGuard Enterprise Server verschlüsselt wird: Sophos-Verschlüsselung oder SSL-Verschlüsselung.

   Der Vorteil bei SSL ist, dass es ein Standardprotokoll ist und eine schnellere Verbindung aufgebaut werden kann als mit der SafeGuard Transportverschlüsselung. SSL-Verschlüsselung wird standardmäßig ausgewählt. Weitere Informationen zur Absicherung von Transportverbindungen mit SSL finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

9. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
10. Klicken Sie auf **Konfigurationspaket erstellen**.

    WennSie als Modus für die **Transportverschlüsselung** die SSL-Verschlüsselung ausgewählt haben, wird die Serververbindung validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Sie müssen das Paket auf den Endpoints verteilen und installieren.

15.2 Erzeugen eines Konfigurationspakets für Standalone-Endpoints

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Standalone Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Geben Sie eine zuvor im SafeGuard Management Center erstellte **Richtliniengruppe** an, die für die Endpoints gelten soll.
6. Unter **POA Gruppe** können Sie eine POA-Gruppe auswählen, die dem Endpoint zugeordnet wird. POA-Benutzer können für administrative Aufgaben auf den Endpoint zugreifen, nachdem die SafeGuard Power-on Authentication aktiviert wurde. Um POA-Benutzer zuzuweisen, müssen Sie die POA-Gruppe zunächst im Bereich **Benutzer & Computer** des SafeGuard Management Center anlegen.
7. Wenn sich das derzeit aktive Unternehmenszertifikat in der SafeGuard Enterprise Datenbank von dem auf den Endpoints, die das neue Konfigurationspaket erhalten sollen, unterscheidet, wählen Sie die relevante **CCO** (Company Certificate Change Order).

   Hinweis: Die Installation des neuen Konfigurationspakets schlägt fehl, wenn die derzeit aktiven Unternehmenszertifikate in der SafeGuard Enterprise Datenbank und auf dem Endpoint nicht übereinstimmen und keine passende **CCO** im Paket enthalten ist.

8. Geben Sie unter **Speicherort für Schlüssel-Sicherungskopie** einen freigegebenen Netzwerkpfad für das Speichern der Schlüssel-Recovery-Datei an oder wählen Sie einen Netzwerkpfad aus. Geben Sie den freigegebenen Pfad in folgender Form ein: `\\network computer\`, zum Beispiel `\\mycompany.edu\`. Wenn Sie hier keinen Pfad angeben, wird der Benutzer beim ersten Anmelden am Endpoint nach der Installation gefragt, wo die Schlüsseldatei gespeichert werden soll.

   Die Schlüssel-Recovery-Datei (XML) wird für die Durchführung von Recovery-Vorgängen bei durch Sophos SafeGuard geschützten Endpoints benötigt. Sie wird auf allen durch Sophos SafeGuard geschützten Endpoints erzeugt.

   Hinweis: Stellen Sie sicher, dass diese Schlüssel-Recovery-Datei an einem Speicherort abgelegt wird, auf den die Mitarbeiter des Helpdesk Zugriff haben. Die Dateien können dem Helpdesk auch durch andere Mechanismen zugänglich gemacht werden. Die Datei ist mit dem Unternehmenszertifikat verschlüsselt. Sie kann also auch auf externen Medien oder auf dem Netzwerk gespeichert werden, um sie dem Helpdesk für Recovery-Vorgänge zur Verfügung zu stellen. Sie kann auch per E-Mail verschickt werden.

9. Geben Sie einen Ausgabepfad für das Konfigurationspaket (MSI) an.
10. Klicken Sie auf **Konfigurationspaket erstellen**.

Das Konfigurationspaket (MSI) wird im angegebenen Verzeichnis angelegt. Sie müssen das Paket auf den Endpoints verteilen und installieren.

15.3 Erzeugen eines Konfigurationspakets für Macs

Ein Konfigurationspaket für einen Mac enthält die relevanten Serverinformationen sowie das Unternehmenszertifikat. Der Mac benutzt diese Informationen zum Zurückmelden von

Statusinformationen (SafeGuard POA an/aus, Verschlüsselungsstatus usw.). Die Statusinformationen werden im SafeGuard Management Center angezeigt.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Managed Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht notwendig).
6. Wählen Sie **SSL** als **Transportverschlüsselung** für die Verbindung zwischen dem Endpoint und dem SafeGuard Enterprise Server. Für Macs wird **Sophos** als **Transportverschlüsselung** nicht unterstützt.
7. Geben Sie einen Ausgabepfad für das Konfigurationspaket (ZIP) an.
8. Klicken Sie auf **Konfigurationspaket erstellen**.

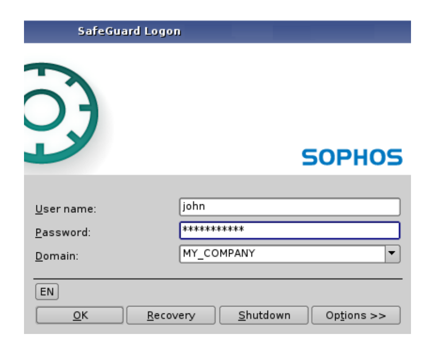
   Die Server-Verbindung für den SSL **Transportverschlüsselung** Modus wird validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (ZIP) wird nun im angegebenen Verzeichnis angelegt. Sie müssen das Paket auf Ihren Macs verteilen und installieren. Siehe auch die Handbücher für *Sophos SafeGuard Native Device Encryption for Mac* und *Sophos SafeGuard File Encryption for Mac*.

16 SafeGuard Enterprise Power-on Authentication (POA)

Hinweis: Diese Beschreibung gilt für Windows 7 Endpoints mit SafeGuard Festplattenverschlüsselung.

SafeGuard Enterprise identifiziert den Benutzer bereits, bevor das Betriebssystem startet. Hierbei startet vorher ein SafeGuard Enterprise eigener Systemkern. Dieser ist gegen Modifikationen geschützt und versteckt auf der Festplatte gespeichert. Erst wenn sich der Benutzer in der SafeGuard POA korrekt authentisiert hat, wird das Betriebssystem (Windows) von der verschlüsselten Partition aus gestartet. Die Anmeldung an Windows erfolgt später automatisch. Analog wird verfahren, wenn sich ein Endpoint im Ruhezustand (Hibernation, Suspend to Disk) befindet und wieder eingeschaltet wird.



Die SafeGuard Power-on Authentication bietet unter anderem folgende Vorteile:

- Grafische Benutzeroberfläche, mit Mausunterstützung und verschiebbaren Fenstern, und damit einfache, übersichtliche Bedienung.
- Vom Firmenkunden per Richtlinie anpassbares grafisches Layout (Hintergrundbild, Anmeldebild, Willkommensmeldung etc.).
- Unterstützung für eine Reihe von Smartcard-Lesegeräten und Smartcards.
- Unterstützung von Windows-Benutzerkonten und Kennwörtern bereits zum Pre-Boot Zeitpunkt, keine separaten Zugangsdaten mehr, die sich der Benutzer merken muss.
- Unterstützung von Unicode und damit auch fremdsprachigen Kennwörtern bzw. Benutzeroberflächen.

16.1 Ablauf der Anmeldung

SafeGuard Enterprise arbeitet mit zertifikatsbasierter Anmeldung. Deswegen benötigt ein Benutzer zur erfolgreichen Anmeldung in der SafeGuard Power-on Authentication Schlüssel und Zertifikate. Benutzerspezifische Schlüssel und Zertifikate werden jedoch erst nach einer erfolgreichen Windows-Anmeldung erzeugt. Nur Benutzer, die sich erfolgreich an Windows angemeldet haben, können sich später auch in der SafeGuard Power-on Authentication authentisieren.

Um den Ablauf der Anmeldung eines Benutzers in SafeGuard Enterprise zu verdeutlichen, im Folgenden eine kurze Einführung. Eine detaillierte Beschreibung der SafeGuard POA-Anmeldevorgänge finden Sie in der *SafeGuard Enterprise Benutzerhilfe*.

SafeGuard Autologon

Nach dem Neustart erscheint bei der ersten Anmeldung am Endpoint der SafeGuard Enterprise Autologon.

Was passiert?

1. Ein Autouser wird angemeldet.
2. Der Computer registriert sich automatisch am SafeGuard Enterprise Server.
3. Der Maschinenschlüssel wird an den SafeGuard Enterprise Server geschickt und in der SafeGuard Enterprise Datenbank abgelegt.
4. Die Maschinenrichtlinien werden an den Endpoint geschickt.

Anmeldung an Windows

Der Windows-Anmeldedialog wird angezeigt. Der Benutzer meldet sich an.

Was passiert?

1. Benutzername und ein Hash-Wert der Benutzerdaten werden an den Server geschickt.
2. Benutzerrichtlinien, Zertifikate und Schlüssel werden erzeugt und an den Endpoint geschickt.
3. Die SafeGuard POA wird aktiviert.

SafeGuard POA-Anmeldung

Nach dem Neustart des Endpoint erscheint die SafeGuard POA.

Was passiert?

1. Zertifikate und Schlüssel für den Benutzer sind vorhanden, und er kann sich in der SafeGuard POA anmelden.
2. Alle Daten sind sicher mit dem öffentlichen RSA Schlüssel des Benutzers verschlüsselt.
3. Alle weiteren Benutzer, die sich anmelden wollen, müssen erst in die SafeGuard POA importiert werden.

16.1.1 Anmeldeverzögerung

Auf einem durch SafeGuard Enterprise geschützten Endpoint tritt eine Anmeldeverzögerung in Kraft, wenn ein Benutzer während der Anmeldung an Windows oder an die SafeGuard Power-on Authentication falsche Anmeldeinformationen eingibt. Mit jedem fehlgeschlagenen Anmeldeversuch verlängert sich jeweils die Anmeldeverzögerung. Nach einer fehlgeschlagenen Anmeldung erscheint ein Dialog, der die verbleibende Verzögerungszeit anzeigt.

Hinweis: Wenn ein Benutzer während der Anmeldung mit Token eine falsche PIN eingibt, tritt keine Anmeldeverzögerung ein.

Sie können die Anzahl an erlaubten Anmeldeversuchen in einer Richtlinie vom Typ **Authentisierung** über die Option **Maximalanzahl von erfolglosen Anmeldeversuchen** festlegen. Wenn die Maximalanzahl an erfolglosen Anmeldeversuchen erreicht ist, wird der Endpoint gesperrt. Um eine Computersperre aufzuheben, kann der Benutzer ein Challenge/Response-Verfahren starten.

16.2 Registrieren weiterer SafeGuard Enterprise-Benutzer

Der erste Benutzer, der sich in Windows anmeldet, ist automatisch in der SafeGuard POA registriert. Zunächst kann sich kein weiterer Windows-Benutzer in der SafeGuard POA anmelden.

Weitere Benutzer müssen mit Hilfe des ersten Benutzers importiert werden. Eine detaillierte Beschreibung zum Importieren weiterer Benutzer finden Sie in der SafeGuard Enterprise Benutzerhilfe.

Eine Richtlinieneinstellung legt fest, wer einen neuen Benutzer importieren darf. Sie finden diese Richtlinie im SafeGuard Management Center unter

Richtlinien

- Typ: **Spezifische Computereinstellungen**
- Feld: **Registrieren von neuen SGN-Benutzern erlauben**

Standardeinstellung: **Besitzer**

Wer der Besitzer eines Endpoint ist, wird im SafeGuard Management Center festgelegt unter

Benutzer und Computer

- <Endpoint-Name> markieren
- Registerkarte **Benutzer**

16.3 Benutzertypen

Es gibt verschiedene Benutzertypen in SafeGuard Enterprise. Weitere Informationen darüber, wie das Standardverhalten dieser Benutzertypen geändert werden kann, finden Sie unter Richtlinieneinstellungen (Seite 126).

- **Besitzer:** Der Benutzer, der sich als erster nach der Installation von SafeGuard Enterprise an einem Endpoint anmeldet, wird nicht nur als SGN-Benutzer eingetragen, sondern auch als Besitzer dieses Endpoints. Sofern die Standardeinstellungen nicht geändert wurden, kann der Besitzer es anderen Benutzern ermöglichen, sich an dem Endpoint anzumelden und SGN-Benutzer zu werden.
- **SGN-Benutzer:** Ein „vollwertiger“ SGN-Benutzer kann sich bei der SafeGuard Power-on Authentication anmelden, wird der UMA (User Machine Assignment - Benutzer-Computer Zuordnung) hinzugefügt und erhält ein Benutzerzertifikat und einen Schlüsselring für den Zugriff auf verschlüsselte Daten.
- **SGN Windows-Benutzer:** Ein SGN Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er wie ein SGN-Benutzer auf verschlüsselte Dateien zugreifen kann. Er wird auch der UMA hinzugefügt, d. h. er darf sich auf diesem Endpoint bei Windows anmelden.

- **SGN-Gastbenutzer:** Ein SGN-Gastbenutzer wird nicht der UMA hinzugefügt, erhält keine Berechtigung zum Anmelden bei der SafeGuard POA, bekommt kein Zertifikat und keinen Schlüsselring zugewiesen und wird nicht in der Datenbank gespeichert. Unter Spezifische Computereinstellungen - Grundeinstellungen (Seite 156) finden Sie Informationen darüber, wie verhindert wird, dass sich SGN-Gastbenutzer bei Windows anmelden.

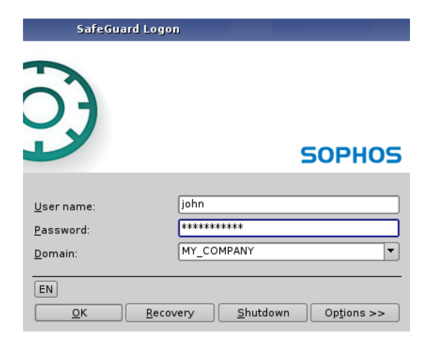
- **Service Account:** Mit Service Accounts können sich Benutzer (z. B. Mitarbeiter des IT-Teams, Rollout-Beauftragte) nach der Installation von SafeGuard Enterprise an Endpoints anmelden, ohne die SafeGuard POA zu aktivieren und ohne dass sie als SGN-Benutzer (Besitzer) zu den Endpoints hinzugefügt werden. Benutzer, die in eine Service Account-Liste aufgenommen wurden, werden nach ihrer Windows-Anmeldung am Endpoint als SGN-Gastbenutzer behandelt.

- **POA-Benutzer:** Nach Aktivierung der POA ist es unter Umständen noch erforderlich, administrative Aufgaben auszuführen. POA-Benutzer sind vordefinierte lokale Konten, die die POA absolvieren dürfen. Es findet keine automatische Anmeldung bei Windows statt. Benutzer, die sich mit POA-Benutzerkonten anmelden, melden sich bei Windows mit ihren bestehenden Windows-Konten an. Diese Benutzerkonten werden im Bereich **Benutzer & Computer** des SafeGuard Management Center definiert (Benutzername und Kennwort) und werden dem Endpoint in POA-Gruppen zugewiesen. Weitere Informationen finden Sie unter POA -Benutzer für die SafeGuard POA-Anmeldung (Seite 120).

16.4 Konfigurieren der SafeGuard Power-on Authentication

Der SafeGuard POA-Dialog besteht aus folgenden Komponenten:

- Anmeldebild
- Dialogtexte
- Sprache des Tastaturlayouts



Das Erscheinungsbild des SafeGuard POA-Dialogs können Sie über Richtlinieneinstellungen im SafeGuard Management Center an Ihre jeweiligen Anforderungen anpassen.

16.4.1 Hintergrund- und Anmeldebild

In der Standardeinstellung werden Bilder im SafeGuard-Design als Hintergrund- und Anmeldebild angezeigt. Es ist jedoch möglich, andere Bilder anzuzeigen, z. B. ein Firmenlogo.

Hintergrund- und Anmeldebilder werden über eine Richtlinie vom Typ **Allgemeine Einstellungen** festgelegt.

Hintergrund- und Anmeldebilder müssen bestimmten Anforderungen entsprechen, damit sie in SafeGuard Enterprise verwendet werden können:

Hintergrundbild in der POA

Maximale Dateigröße für alle Hintergrundbilder: **500 KB**

SafeGuard Enterprise unterstützt für Hintergrundbilder zwei Varianten:

- **1024x768** (VESA-Modus)

  Farben: keine Einschränkung

  Richtlinie vom Typ **Allgemeine Einstellungen**, Option **Hintergrundbild in der POA.**

- **640 x 480** (VGA-Modus)

  Farben: 16

  Richtlinie vom Typ **Allgemeine Einstellungen**, Option **Hintergrundbild in der POA (niedrige Auflösung)**

Anmeldebild

Maximale Dateigröße für alle Anmeldebilder: **100 KB**

SafeGuard Enterprise unterstützt für Anmeldebilder zwei Varianten:

- **413x140**

  Farben: keine Einschränkung

  Richtlinie vom Typ **Allgemeine Einstellungen**, Option **Anmeldebild in der POA**

- **413x140**

  Farben: 16

  Richtlinie vom Typ **Allgemeine Einstellungen**, Option **Anmeldebild in der POA (niedrige Auflösung)**

Bilder müssen zunächst als Dateien (BMP, PNG, JPG) erstellt werden und können dann im Navigationsbereich registriert werden.

16.4.1.1 Registrieren von Bildern

1. Klicken Sie im **Richtlinien** Navigationsbereich mit der rechten Maustaste auf **Bilder** und wählen Sie **Neu > Bild**.
2. Geben Sie unter **Bildname** einen Namen für das Bild ein.
3. Wählen Sie über die Schaltfläche **[...]** das zuvor erstellte Bild aus.
4. Klicken Sie auf **OK**.

Das neue Bild wird als Unterknoten des Eintrags **Bilder** im Richtlinien-Navigationsbereich angezeigt. Ist ein Bild markiert, wird es im Aktionsbereich angezeigt. Das Bild kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Sie können so weitere Bilder registrieren. Alle registrierten Bilder werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Bild ändern** können Sie das zugeordnete Bild austauschen.

16.4.2 Benutzerdefinierter Informationstext in der SafeGuard POA

Sie können in der SafeGuard POA folgende **benutzerdefinierte Informationstexte** anzeigen lassen:

- Infotext beim Starten eines Challenge/Response-Verfahrens zur Hilfe bei der Anmeldung (z. B.: “Bitte rufen Sie Ihren Support unter der Telefonnummer 01234-56789 an.”).

  Mit der Option **Texte** in einer Richtlinie des Typs **Allgemeine Einstellungen** können Sie einen Informationstext definieren.

- Rechtliche Hinweise, die nach der Anmeldung an der SafeGuard POA angezeigt werden.

  Mit der Option **Text für rechtliche Hinweise** in einer Richtlinie des Typs **Spezifische Computereinstellungen** können Sie einen Text für rechtliche Hinweise definieren.

- Text mit zusätzlichen Informationen, der nach der Anmeldung an der SafeGuard POA angezeigt werden soll.

  Mit der Option **Text für zusätzliche Informationen** in einer Richtlinie des Typs **Spezifische Computereinstellungen** können Sie einen Text für zusätzliche Informationen definieren.

16.4.2.1 Registrieren von Informationstexten

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Informationstexte beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden sie bei der Registrierung automatisch in dieses Format konvertiert. Bei der Verwendung von Sonderzeichen in den Informationstexten für die SafeGuard POA sollte vorsichtig vorgegangen werden. Einige dieser Zeichen werden u. U. nicht korrekt dargestellt.

So registrieren Sie Informationstexte:

1. Klicken Sie im **Richtlinien**-Navigationsbereich mit der rechten Maustaste auf **Texte** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.
3. Klicken Sie auf **[...]** um die zuvor erstellte Textdatei auszuwählen. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Texte** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich auf der rechten Seite angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Wenn Sie auf diese Schaltfläche klicken, wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

16.4.3 Sprache der SafeGuard POA-Dialogtexte

Alle Texte in der SafeGuard POA werden nach der Installation der SafeGuard Enterprise Verschlüsselungssoftware mit den Standardeinstellungen in der Sprache angezeigt, die bei der Installation von SafeGuard Enterprise in den Regions- und Sprachoptionen von Windows als Standardsprache am Endpoint eingestellt ist.

Sie können die Sprache der SafeGuard POA-Dialogtexte nach der Installation von SafeGuard Enterprise mit einer der beide folgenden Methoden umstellen:

- Ändern Sie die Standardsprache in den Windows Regions- und Sprachoptionen auf dem Endpoint. Nachdem der Benutzer den Endpoint zweimal neu gestartet hat, ist die neue Spracheinstellung in der SafeGuard POA aktiv.

- Erstellen Sie eine Richtlinie des Typs **Allgemeine Einstellungen**, legen Sie die Sprache im Feld **Sprache am Client** fest und übertragen Sie die Richtlinie auf den Endpoint.

Hinweis: Wenn Sie eine Richtlinie erstellen und sie an den Endpoint übertragen, gilt die in der Richtlinie festgelegte Sprache anstelle der in den Windows Regions- und Sprachoptionen angegebenen Sprache.

16.4.4 Tastaturlayout

Beinahe jedes Land hat ein eigenes Tastaturlayout. In der SafeGuard POA macht sich das Tastaturlayout bei der Eingabe von Benutzernamen, Kennwort und Response Code bemerkbar.

SafeGuard Enterprise übernimmt standardmässig das Tastaturlayout in die SafeGuard POA, das zum Zeitpunkt der Installation in den Regions- und Sprachoptionen von Windows gesetzt ist. Ist unter Windows „Deutsch“ als Tastaturlayout gesetzt, wird in der SafeGuard POA das deutsche Tastaturlayout verwendet.

Die Sprache des verwendeten Tastaturlayouts wird in der SafeGuard POA angezeigt, z. B. „EN“ für Englisch. Neben dem Standard-Tastaturlayout kann das US-Tastaturlayout (Englisch) gewählt werden.

Es gibt bestimmte Ausnahmefälle:

- Das Tastaturlayout wird zwar unterstützt, aufgrund fehlender Schriften (z. B. bei Bulgarisch) werden im Feld **Benutzername** aber nur Sonderzeichen angezeigt.

- Es ist kein spezielles Tastaturlayout verfügbar (z. B. Dominikanische Republik). In solchen Fällen greift die SafeGuard POA auf das Original-Tastaturlayout zurück. Für die Dominikanische Republik ist dies „Spanisch“.

- Wenn Benutzername oder Kennwort aus Zeichen bestehen, die vom ausgewählten Tastaturlayout oder dem Original-Tastaturlayout nicht unterstützt werden, kann sich der Benutzer nicht an der SafeGuard POA anmelden.

Hinweis: Alle nicht unterstützten Tastaturlayouts verwenden als Standard das US-Tastaturlayout. Das bedeutet, dass auch nur Zeichen erkannt und eingegeben werden können, die im US-Tastaturlayout unterstützt werden. Benutzer können sich demnach nur an der SafeGuard POA anmelden, wenn ihre Benutzernamen und Kennwörter sich aus Zeichen zusammensetzen, die vom US-Tastaturlayout oder dem entsprechenden Original-Layout unterstützt werden.

Virtuelle Tastatur

SafeGuard Enterprise bietet die Möglichkeit, in der SafeGuard POA eine virtuelle Tastatur anzeigen zu lassen. Der Benutzer kann dann z. B. Anmeldeinformationen durch Klick auf die am Bildschirm angezeigten Tasten eingeben.

Als Sicherheitsbeauftragter können Sie die Anzeige der virtuellen Tastatur in einer Richtlinie vom Typ **Spezifische Computereinstellungen** über die Option **Virtuelle Tastatur in der POA** aktivieren/deaktivieren.

Die Unterstützung der virtuellen Tastatur muss über eine Richtlinieneinstellung aktiviert/deaktiviert werden.

Für die virtuelle Tastatur werden verschiedene Layouts angeboten und das Layout kann mit den gleichen Einstellungen wie das normale Tastaturlayout geändert werden.

16.4.4.1 Ändern des Tastaturlayouts

Das normale einschließlich des virtuellen Tastaturlayouts der SafeGuard Power-on Authentication kann nachträglich geändert werden.

1. Wählen Sie **Start > Systemsteuerung > Regions- und Sprachoptionen > Erweitert**.
2. Wählen Sie auf der Registerkarte **Regionale Einstellungen** die gewünschte Sprache aus.
3. Wählen Sie dann auf der Registerkarte **Erweitert** unter **Standardeinstellungen für Benutzerkonten** die Option **Alle Einstellungen auf das aktuelle Benutzerkonto und Standardbenutzerprofil anwenden**.
4. Klicken Sie auf **OK**.

Die SafeGuard POA merkt sich das bei der letzten erfolgreichen Anmeldung verwendete Tastaturlayout und aktiviert dieses beim nächsten Anmelden automatisch. Hierzu sind zwei Neustarts des Endpoint notwendig. Wenn dieses gemerkte Tastaturlayout über die **Regions- und Sprachoptionen** abgewählt wird, bleibt es dem Anwender noch so lange erhalten, bis er eine andere Sprache ausgewählt hat.

Hinweis: Zusätzlich ist es notwendig, die Sprache des Tastatur-Layouts für andere, nicht-Unicode-Programme, zu ändern.

Falls die gewünschte Sprache nicht auf dem Endpoint vorhanden ist, werden Sie von Windows evtl. aufgefordert, die Sprache zu installieren. Danach müssen Sie den Endpoint zweimal neu starten, damit das neue Tastaturlayout von der SafeGuard Power-on Authentication eingelesen und dann auch über diese eingestellt werden kann.

Sie können das gewünschte Tastaturlayout der SafeGuard Power-on Authentication mit der Maus oder mit der Tastatur (**Alt+Shift**) ändern.

Sie können über **`Start > Ausführen > regedit > HKEY_USERS\.DEFAULT\Keyboard Layout\Preload`** einsehen, welche Sprachen auf dem System installiert und damit verfügbar sind.

16.5 In der SafeGuard Power-on Authentication unterstützte Hotkeys

Bestimmte Hardware-Einstellungen und -Funktionalitäten können Probleme beim Starten des Endpoint verursachen, die dazu führen, dass der Rechner im Startvorgang hängen bleibt. Die SafeGuard Power-on Authentication unterstützt eine Reihe von Hotkeys, mit denen sich Hardware-Einstellungen und Funktionalitäten modifizieren lassen. Darüber hinaus sind in die

auf dem Endpoint zu installierende .MSI-Datei Grey Lists und Black Lists integriert, die Funktionen abdecken, von denen ein solches Problemverhalten bekannt ist.

Wir empfehlen, vor jeder größer angelegten SafeGuard Enterprise Installation die aktuelle Version der SafeGuard POA-Konfigurationsdatei zu installieren. Die Datei wird monatlich aktualisiert und steht hier zum Download zur Verfügung:
http://www.sophos.com/de-de/support/knowledgebase/110285.aspx

Sie können diese Datei anpassen, um die Hardware einer spezifischen Umgebung abzudecken.

Hinweis: Wenn Sie eine angepasste Datei definieren, wird nur diese verwendet, nicht die in der .msi-Datei integrierte Datei. Die Standarddatei wird nur angewendet, wenn keine SafeGuard POA-Konfigurationsdatei definiert ist oder keine gefunden wird.

Um die SafeGuard POA-Konfigurationsdatei zu installieren, geben Sie folgenden Befehl ein:

```
MSIEXEC /i <Client-MSI-Paket> POACFG=<Pfad der SafeGuard
POA-Konfigurationsdatei>
```

Sie können uns bei der Optimierung der Hardware-Kompatibilität unterstützen, indem Sie ein von uns zur Verfügung gestelltes Tool ausführen. Dieses Tool liefert ausschließlich Hardware-relevante Informationen. Das Tool ist einfach zu bedienen. Die gesammelten Informationen werden zur Hardware-Konfigurationsdatei hinzugefügt.

Für weitere Informationen, siehe
http://www.sophos.com/de-de/support/knowledgebase/110285.aspx.

Die folgenden Hotkeys werden in der SafeGuard POA unterstützt:

- **Shift F3** = USB Legacy Unterstützung (An/Aus)
- **Shift F4** = VESA Grafikmodus (Aus/An)
- **Shift F5** = USB 1.x und 2.0 Unterstützung (Aus/An)
- **Shift F6** = ATA Controller (Aus/An)
- **Shift F7** = nur USB 2.0 Unterstützung (Aus/An)

  USB 1.x Unterstützung bleibt wie über Shift F5 gesetzt.
- **Shift F9** = ACPI/APIC (Aus/An)

USB Hotkeys Abhängigkeitsmatrix

Shift F3	Shift F5	Shift F7	Legacy	USB 1.x	USB 2.0	Anmerkung
aus	aus	aus	an	an	an	3.
an	aus	aus	aus	an	an	Standard
aus	an	aus	an	aus	aus	1., 2.
an	an	aus	an	aus	aus	1., 2.
aus	aus	an	an	an	aus	3.
an	aus	an	aus	an	aus	

Shift F3	Shift F5	Shift F7	Legacy	USB 1.x	USB 2.0	Anmerkung
aus	an	an	an	aus	aus	
an	an	an	an	aus	aus	2.

1. Shift F5 deaktiviert sowohl die Unterstützung von USB 1.x als auch von USB 2.0.

   Hinweis: Wenn Sie Shift F5 drücken, reduziert sich die Wartezeit bis zum Starten der SafeGuard POA erheblich. Beachten Sie jedoch, dass bei Benutzung einer USB-Tastatur oder einer USB-Maus am betreffenden Computer diese Geräte durch Drücken von **Shift F5** möglicherweise deaktiviert werden.

2. Wenn die USB-Unterstützung nicht aktiviert ist, versucht die SafeGuard POA, BIOS SMM zu benutzen anstatt den USB-Controller zu sichern und wiederherzustellen. Der Legacy-Modus kann in diesem Szenario funktionieren.

3. Die Legacy-Unterstützung ist aktiviert, die USB-Unterstützung ist aktiviert. Die SafeGuard POA versucht, den USB-Controller zu sichern und wiederherzustellen. Der Computer kann sich je nach eingesetzter BIOS-Version aufhängen.

Es besteht die Möglichkeit, Änderungen, die über Hotkeys vorgenommen werden können, bei der Installation der SafeGuard Enterprise Verschlüsselungssoftware über eine mst Datei bereits vorzudefinieren. Verwenden Sie dazu den entsprechenden Aufruf in Verbindung mit msiexec.

NOVESA	Bestimmt, ob VESA- oder VGA-Modus verwendet wird: 0 = VESA-Modus (Standard), 1 = VGA-Modus
NOLEGACY	Bestimmt, ob nach der SafeGuard POA-Anmeldung Legacy-Unterstützung aktiviert ist: 0 = Legacy-Unterstützung aktiviert, 1 = Legacy-Unterstützung nicht aktiviert (Standard)
ALTERNATE:	Bestimmt, ob USB-Geräte von der SafeGuard POA unterstützt werden: 0 = USB-Unterstützung ist aktiviert (Standard), 1 = keine USB-Unterstützung
NOATA	Bestimmt, ob der int13-Gerätetreiber verwendet wird: 0 = Standard-ATA-Gerätetreiber (Standard), 1 = Int13-Gerätetreiber
ACPIAPIC	Bestimmt, ob ACPI/APIC-Unterstützung verwendet wird: 0 = keine ACPI/APIC-Unterstützung (Standard), 1 = ACPI/APIC-Unterstützung aktiv

16.6 Deaktivierte SafeGuard POA und Lenovo Rescue and Recovery

Sollte auf dem Computer die SafeGuard Power-on Authentication deaktiviert sein, so sollte zum Schutz vor dem Zugriff auf verschlüsselte Dateien aus der Rescue and Recovery Umgebung heraus die Rescue and Recovery Authentisierung eingeschaltet sein.

Detaillierte Informationen zur Aktivierung der Rescue and Recovery Authentisierung finden Sie in der Lenovo Rescue and Recovery Dokumentation.

17 Administrative Zugangsoptionen für Endpoints

Hinweis: Die folgenden Beschreibungen beziehen sich auf Windows Endpoints, die mit SafeGuard Enterprise mit SafeGuard Power-on Authentication geschützt sind.

Um es Benutzern zu ermöglichen, sich nach der Installation von SafeGuard Enterprise zur Durchführung von administrativen Aufgaben an Endpoints anzumelden, bietet SafeGuard Enterprise zwei verschiedene Benutzerkontotypen.

- **Service Accounts für die Windows-Anmeldung**

  Mit Service Accounts können sich Benutzer (z. B. Rollout-Beauftragte, Mitglieder des IT-Teams) nach der Installation von SafeGuard Enterprise an Endpoints anmelden (Windows-Anmeldung), ohne die SafeGuard Power-on Authentication zu aktivieren. Die Benutzer werden auch nicht als SafeGuard Enterprise Benutzer zum Endpoint hinzugefügt. Service Account Listen werden im Bereich **Richtlinien** des SafeGuard Management Center angelegt und über Richtlinien den Endpoints zugewiesen. Benutzer, die in eine Service Account Liste aufgenommen wurden, werden bei der Anmeldung am Endpoint als Gastbenutzer behandelt.

  Hinweis: Service Account Listen werden den Endpoints über Richtlinien zugewiesen. Sie sollten bereits im ersten SafeGuard Enterprise Konfigurationspaket, das Sie für die Konfiguration der Endpoints erstellen, enthalten sein.

  Weitere Informationen finden Sie unter Service Account-Listen für die Windows-Anmeldung (Seite 115).

- **POA-Benutzer für die Anmeldung an der SafeGuard POA**

  POA-Benutzer sind vordefinierte lokale Benutzerkonten, die es Benutzern (z. B. Mitgliedern des IT-Teams) ermöglichen, sich nach der Aktivierung der SafeGuard POA an Endpoints zur Ausführung administrativer Aufgaben anzumelden (SafeGuard POA-Anmeldung). Diese Benutzerkonten werden im Bereich **Benutzer & Computer** des SafeGuard Management Center definiert (Benutzername und Kennwort) und werden den Endpoints über POA-Gruppen in Konfigurationspaketen zugewiesen.

  Weitere Informationen finden Sie unter POA -Benutzer für die SafeGuard POA-Anmeldung (Seite 120).

18 Service Account Listen für die Windows-Anmeldung

Hinweis: Service Accounts werden nur von Windows Endpoints unterstützt, die von SafeGuard Enterprise mit SafeGuard Power-on Authentication geschützt werden.

Bei den meisten Implementationen von SafeGuard Enterprise installiert zunächst ein Rollout-Team neue Computer in einer Umgebung. Danach folgt die Installation von SafeGuard Enterprise. Zu Installations- und Prüfungszwecken meldet sich der Rollout-Beauftragte dann am jeweiligen Computer an, bevor der Endbenutzer diesen erhält und die Möglichkeit hat, die SafeGuard Power-on Authentication zu aktivieren.

So ergibt sich folgendes Szenario:

1. SafeGuard Enterprise wird auf einem Endpoint installiert.
2. Nach dem Neustart des Endpoint meldet sich der Rollout-Beauftragte an.
3. Der Rollout-Beauftragte wird zur SafeGuard POA hinzugefügt und die POA wird aktiv. Der Rollout-Benutzer wird Besitzer des Endpoint.

Wenn der Endbenutzer den Endpoint erhält, kann er sich nicht an der SafeGuard POA anmelden. Er muss ein Challenge/Response-Verfahren durchführen.

Um zu verhindern, dass administrative Vorgänge auf einem durch SafeGuard Enterprise geschützten Endpoint bewirken, dass die SafeGuard Power-on Authentication aktiviert wird und Rollout-Beauftragte als Benutzer zum Endpoint hinzugefügt werden, ermöglicht SafeGuard Enterprise das Anlegen von Listen mit Service Accounts. Die in den Listen enthaltenen Benutzer werden dadurch als SafeGuard Enterprise Gastbenutzer behandelt

Mit Service Accounts ergibt sich folgendes Szenario:

1. SafeGuard Enterprise wird auf einem Endpoint installiert.
2. Der Endpoint wird neu gestartet und ein Rollout-Beauftragter, der in einer Service Account Liste aufgeführt ist, meldet sich an.
3. Gemäß der auf den Computer angewendeten Service Account Liste wird der Benutzer als Service Account erkannt und als Gastbenutzer behandelt.

Der Rollout-Beauftragte wird nicht zur SafeGuard POA hinzugefügt und die POA wird nicht aktiviert. Der Rollout-Beauftragte wird nicht Besitzer des Endpoint. Der Endbenutzer kann sich anmelden und die SafeGuard POA aktivieren.

Hinweis: Service Account Listen werden den Endpoints über Richtlinien zugewiesen. Sie sollten bereits im ersten SafeGuard Enterprise Konfigurationspaket, das Sie für die Konfiguration der Endpoints erstellen, enthalten sein.

18.1 Anlegen von Service Account Listen und Hinzufügen von Benutzern

1. Klicken Sie im Navigationsbereich auf **Richtlinien**.
2. Markieren Sie im Richtlinien-Navigationsbereich den Eintrag **Service Account Listen**.

3. Klicken Sie im Kontextmenü von **Service Account Listen** auf **Neu > Service Account Liste**.
4. Geben Sie einen Namen für die Service Account Liste ein und klicken Sie auf **OK**.
5. Markieren Sie die neue Liste unter **Service Account Listen** im Richtlinien-Navigationsfenster.
6. Klicken Sie im Arbeitsbereich mit der rechten Maustaste, um das Kontextmenü für die Service Account Liste zu öffnen. Wählen Sie **Hinzufügen** im Kontextmenü.

   Eine neue Benutzerzeile wird hinzugefügt.

7. Geben Sie den **Benutzernamen** und den **Domänennamen** in den entsprechenden Spalten ein und drücken Sie **Enter**. Um weitere Benutzer hinzuzufügen, wiederholen Sie diesen Schritt.
8. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern** Symbol in der Symbolleiste klicken.

Die Service Account Liste ist registriert und kann beim Anlegen einer Richtlinie ausgewählt werden.

18.2 Zusätzliche Informationen zur Eingabe von Benutzer- und Domänennamen

Für die Definition von Benutzern in Service Account Listen in den beiden Feldern **Benutzername** und **Domänenname** gibt es unterschiedliche Vorgehensweisen. Darüber hinaus gelten für die Eingabewerte in diesen Feldern bestimmte Einschränkungen.

Verschiedene Anmeldekombinationen abdecken

Durch die beiden separaten Felder **Benutzername** und **Domänenname** pro Listeneintrag lassen sich alle möglichen Anmeldekombinationen (z. B. „Benutzer@Domäne oder „Domäne\Benutzer“) abdecken.

Um mehrere Kombinationen aus Benutzername und Domänenname anzugeben, können Sie Asterisken (*) als Platzhalter verwenden. Ein * ist als erstes Zeichen, als letztes Zeichen und als einziges Zeichen zulässig.

Zum Beispiel:

- **Benutzername:** Administrator
- **Domänenname:** *

Mit dieser Kombination geben Sie alle Benutzer mit dem Benutzernamen „Administrator“ an, die sich an einem Netzwerk oder an einer beliebigen lokalen Maschine anmelden.

Der vordefinierte Domänenname [LOCALHOST], der in der Dropdownliste des Felds **Domänenname** zur Verfügung steht, steht für die Anmeldung an einem beliebigen lokalen Computer.

Zum Beispiel:

- **Benutzername**: "Admin*"
- **Domänenname**: [LOCALHOST]

Mit dieser Kombination geben Sie alle Benutzer an, deren Benutzernamen mit Admin beginnen und die sich an einer beliebigen lokalen Maschine anmelden.

Benutzer können sich auf verschiedene Art und Weise anmelden.

Zum Beispiel:

- Benutzer: test, Domäne: mycompany
- Benutzer: test, Domäne: mycompany.com.

Da Domänenangaben in Service Account Listen nicht automatisch aufgelöst werden, gibt es drei mögliche Methoden für das korrekte Angeben der Domäne:

- Sie wissen genau, wie sich der Benutzer anmelden wird, und geben die Domäne entsprechend exakt ein.
- Sie erstellen mehrere Einträge in der Service Account Liste.
- Sie verwenden Platzhalter, um alle unterschiedlichen Fälle abzudecken (Benutzer: test, Domäne: mycompany*).

Hinweis: Windows verwendet möglicherweise nicht dieselbe Zeichenfolge und kürzt Namen ab. Um dadurch entstehende Probleme zu vermeiden, empfehlen wir, den FullQualifiedName und den Netbios-Namen einzugeben oder Platzhalter zu verwenden.

Einschränkungen

Asterisken sind nur als erstes, letztes und einziges Zeichen zulässig. Beispiele für gültige und ungültige Zeichenfolgen:

- Gültige Zeichenfolgen sind z. B.: Admin*, *, *strator, *minis*.
- Ungültige Zeichenfolgen sind z. B.: **, Admin*trator, Ad*minst*.

Darüber hinaus gelten folgende Einschränkungen:

- Das Zeichen ? ist in Benutzernamen nicht zulässig.
- Die Zeichen / \ [ ] : ; | = , + * ? < > " sind in Domänennamen nicht zulässig.

18.3 Bearbeiten und Löschen von Service Account Listen

Als Sicherheitsbeauftragter mit der Berechtigung **Service Account Listen ändern** können Sie Service Account Listen jederzeit bearbeiten oder löschen:

- Um eine Service Account Liste zu bearbeiten, klicken Sie auf der Liste im Richtlinien-Navigationsfenster. Die Service Account Liste wird im Aktionsbereich geöffnet und Sie können Benutzernamen zufügen, löschen oder ändern.
- Um eine Service Account Liste zu löschen, wählen Sie die Liste im Richtlinien-Navigationsfenster aus, öffnen Sie das Kontextmenü und wählen Sie **Löschen**.

18.4 Zuweisen einer Service Account Liste in einer Richtlinie

1. Legen Sie eine Richtlinie vom Typ **Authentisierung** an oder wählen Sie eine bereits vorhandene aus.
2. Wählen Sie unter **Anmeldeoptionen** die gewünschte Service Account Liste aus der Dropdownliste des Felds **Service Account Liste** aus.

   Hinweis: Die Standardeinstellung dieses Felds ist **[Keine Liste]**, d. h. es gilt keine Service Account Liste. Rollout-Beauftragte, die sich nach der Installation von SafeGuard Enterprise an dem Endpoint anmelden, werden somit nicht als Gastbenutzer behandelt und können die SafeGuard Power-on Authentication aktivieren sowie zum Endpoint hinzugefügt werden. Um die Zuweisung einer Service Account Liste rückgängig zu machen, wählen Sie die Option **[Keine Liste]**.

3. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern** Symbol in der Symbolleiste klicken.

Sie können die Richtlinie nun an die Endpoints übertragen, um die Service Accounts auf den Endpoints zur Verfügung zu stellen.

Hinweis: Wenn Sie unterschiedliche Service Account Listen in verschiedenen Richtlinien auswählen, die alle nach dem RSOP (Resulting Set of Policies, die für einen bestimmten Computer/eine bestimmte Gruppe geltenden Einstellungen) relevant sind, setzt die Service Account Liste in der zuletzt angewandten Richtlinie alle zuvor zugewiesenen Service Account Listen außer Kraft. Service Account Listen werden nicht zusammengeführt. Um das RSOP unter **Benutzer & Computer** einzusehen, brauchen Sie zumindest das Zugriffsrecht **Schreibgeschützt** für die relevanten Objekte.

18.5 Übertragen der Richtlinie an den Endpoint

Service Account Listen sind während der Installation in der Rollout-Phase einer Implementation besonders hilfreich und wichtig. Es wird daher empfohlen, die Service Account Einstellungen unmittelbar nach der Installation an den Endpoint zu übertragen. Um die Service Account Liste zu diesem Zeitpunkt auf dem Endpoint zur Verfügung zu stellen, nehmen Sie in das erste Konfigurationspaket, das Sie zur Konfiguration des Endpoint nach der Installation erstellen, eine Richtlinie vom Typ **Authentisierung** mit den entsprechenden Einstellungen auf.

Sie können die Einstellungen für die Service Account Liste jederzeit ändern, eine neue Richtlinie erstellen und diese an die Endpoints übertragen.

18.6 Anmeldung auf einem Endpoint mit einem Service Account

Bei der ersten Windows-Anmeldung nach dem Neustart des Endpoint meldet sich ein Benutzer, der auf einer Service Account Liste aufgeführt ist, an dem Endpoint als SafeGuard Enterprise Gastbenutzer an. Diese erste Windows-Anmeldung an diesem Endpoint löst weder eine ausstehende Aktivierung der SafeGuard Power-on Authentication aus, noch wird durch die Anmeldung der Benutzer zum Endpoint hinzugefügt. Das SafeGuard Enterprise System Tray Icon zeigt in diesem Fall auch nicht den Balloon Tool Tip „Initialer Benutzerabgleich abgeschlossen“ an.

Anzeige des Service Account Status auf dem Endpoint

Der Gastbenutzer-Anmeldestatus wird auch über das System Tray Icon angezeigt. Weitere Informationen zum System Tray Icon finden Sie in der *SafeGuard Enterprise Benutzerhilfe*, Kapitel *System Tray Icon und Balloon-Ausgabe* (Beschreibung des **SGN-Benutzerstatus** Felds).

18.7 Protokollierte Ereignisse

Die in Zusammenhang mit Service Account Listen durchgeführten Aktionen werden über die folgenden Ereignisse protokolliert:

SafeGuard Management Center

- Service Account Liste <Name> angelegt.
- Service Account Liste <Name> geändert.
- Service Account Liste <Name> gelöscht.

Durch SafeGuard Enterprise geschützte Endpoints

- Windows-Benutzer <Domäne/Benutzer> hat sich um <Zeit> an Maschine <Domäne/Computer> als SGN Service Account angemeldet.
- Neue Service Account Liste importiert.
- Service Account Liste <Name> gelöscht.

19 POA-Benutzer für die Anmeldung an der SafeGuard POA

Hinweis: POA-Benutzer werden nur von Windows Endpoints unterstützt, die von SafeGuard Enterprise mit SafeGuard Power-on Authentication geschützt werden.

Nach der Installation von SafeGuard Enterprise und der Aktivierung der SafeGuard Power-on Authentication (POA), kann der Zugang zu Endpoints für administrative Aufgaben notwendig sein. Mit POA-Benutzern können sich Benutzer (z. B. Mitglieder des IT-Teams) zur Durchführung von administrativen Aufgaben an der SafeGuard Power-on Authentication anmelden, ohne ein Challenge/Response-Verfahren durchführen zu müssen. Eine automatische Anmeldung an Windows erfolgt nicht. Die Benutzer müssen sich an Windows mit ihren vorhandenen Windows-Benutzerkonten anmelden.

Sie können POA-Benutzer anlegen, diese in POA-Gruppen gruppieren und die Gruppen den Endpoints zuweisen. Die Benutzer, die in der POA-Gruppe enthalten sind, werden zur SafeGuard POA hinzugefügt und können sich mit Ihrem vordefinierten Benutzernamen und Kennwort an der POA anmelden.

Hinweis: Für die Verwaltung von POA-Benutzern und POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

19.1 Erstellen von POA-Benutzern

Für das Erstellen von POA-Benutzern und POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA** den Knoten **POA-Benutzer**.
3. Klicken Sie im **POA-Benutzer** Kontextmenü auf **Neu > Neuen Benutzer erstellen**.

   Der Dialog **Neuen Benutzer erstellen** wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen (den Anmeldenamen) für den neuen POA-Benutzer ein.
5. Optional können Sie eine Beschreibung für den neuen POA-Benutzer eingeben.
6. Geben Sie ein Kennwort für den neuen POA-Benutzer ein und bestätigen Sie es.

   Hinweis: Aus Sicherheitsgründen sollte das Kennwort bestimmten Mindest-Komplexitätsanforderungen entsprechen. Zum Beispiel sollte es eine Mindestlänge von 8 Zeichen haben und sowohl aus numerischen als auch alphanumerischen Zeichen bestehen. Ist das hier eingegebene Kennwort zu kurz, so wird eine entsprechende Warnungsmeldung angezeigt.

7. Klicken Sie auf **OK**.

Der neue POA-Benutzer wird angelegt und unter **POA-Benutzer** im **Benutzer & Computer** Navigationsbereich angezeigt.

19.2 Ändern des Kennworts für einen POA-Benutzer

Für das Bearbeiten von POA-Benutzern und POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Benutzer** den relevanten POA-Benutzer.
3. Wählen Sie im Kontextmenü des POA-Benutzers den Befehl **Eigenschaften**.

   Der Eigenschaften-Dialog für den POA-Benutzer wird angezeigt.

4. Geben Sie in der Registerkarte **Allgemein** unter **Benutzerkennwort** das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **OK**.

Für den relevanten POA-Benutzer gilt das neue Kennwort.

19.3 Löschen von POA-Benutzern

Für das Löschen von POA-Benutzern und POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Benutzer** den relevanten POA-Benutzer.
3. Klicken Sie mit der rechten Maustaste auf den POA-Benutzer und wählen Sie **Löschen** aus dem Kontextmenü.

Der POA-Benutzer wird gelöscht. Es wird nicht mehr im **Benutzer & Computer** Navigationsfenster angezeigt.

Hinweis: Wenn der Benutzer einer oder mehreren POA-Gruppen angehört, wird er auch aus allen Gruppen entfernt. Der POA-Benutzer steht jedoch noch so lange auf dem Endpoint zur Verfügung, bis die Zuweisung der POA-Gruppe aufgehoben wird.

19.4 Erstellen von POA-Gruppen

Für das Erstellen von POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

Damit die POA-Gruppen Endpoints zugewiesen werden können, müssen sie in Gruppen zusammengefasst werden.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsbereich unter **POA** den Knoten **POA-Gruppen**.
3. Klicken Sie im **POA-Gruppen** Kontextmenü auf **Neu > Neue Gruppe erstellen**.

   Der **Neue Gruppe erstellen** Dialog wird angezeigt.

4. Geben Sie im Feld **Vollständiger Name** einen Namen für die neue POA-Gruppe ein.

5. Geben Sie optional eine Beschreibung ein.
6. Klicken Sie auf **OK**.

Die neue POA-Gruppe ist angelegt. Sie wird unter **POA-Gruppen** im **Benutzer & Computer** Navigationsfenster angezeigt. Sie können nun POA-Benutzer zur Gruppe hinzufügen.

19.5 Hinzufügen von Benutzern zu POA-Gruppen

Für das Bearbeiten von POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Gruppe** die relevante POA-Gruppe.

   Im Aktionsbereich des SafeGuard Management Center auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt

3. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Hinzufügen** Symbol (grünes Pluszeichen).

   Der **Mitgliedobjekt auswählen** Dialog wird angezeigt

4. Wählen Sie den Benutzer, den Sie zur Gruppe hinzufügen möchten.
5. Klicken Sie auf **OK**.

Der POA-Benutzer wird zur Gruppe hinzugefügt und in der Registerkarte **Mitglieder** angezeigt.

19.6 Entfernen von Benutzern aus POA-Gruppen

Für das Bearbeiten von POA-Gruppen benötigen Sie das Zugriffsrecht **Voller Zugriff** für den **POA** Knoten unter **Benutzer & Computer**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsfenster unter **POA**, **POA-Gruppe** die relevante POA-Gruppe.

   Im Aktionsbereich des SafeGuard Management Center auf der rechten Seite wird die **Mitglieder** Registerkarte angezeigt

3. Wählen Sie den Benutzer, den Sie aus der Gruppe entfernen möchten.
4. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Löschen** Symbol (rotes Kreuzzeichen).

Der Benutzer wird aus der Gruppe entfernt.

19.7 Zuweisen von POA-Benutzern zu Endpoints

Hinweis: Damit die POA-Gruppen Endpoints zugewiesen werden können, müssen sie in Gruppen zusammengefasst werden.

Wie Sie POA-Benutzer Endpoints zuweisen, hängt vom Endpoint-Typ ab:

- Für **zentral verwaltete Endpoints** können POA-Gruppen im Bereich **Benutzer & Computer** in der Registerkarte **POA-Gruppen-Zuweisung** zugewiesen werden.

- Für **Standalone-Endpoints**, die im Standalone-Modus laufen und keine Verbindung zum SafeGuard Enterprise Server haben, muss ein Konfigurationspaket mit einer POA-Gruppe erstellt und an die Computer verteilt werden.

19.7.1 Zuweisen von POA-Benutzern zu zentral verwalteten Endpoints

Um POA-Benutzer zu zentral verwalteten Endpoints zuzuweisen, benötigen Sie die Zugriffsrechte **Voller Zugriff** oder **Schreibgeschützt** für die relevante POA-Gruppe sowie das Zugriffsrecht **Voller Zugriff** für die relevanten Container.

Hinweis: Das Zuweisen von POA-Benutzern wird nur für zentral verwaltete SafeGuard Enterprise Endpoints ab Version 5.60 unterstützt.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Wählen Sie im **Benutzer & Computer** Navigationsbereich den gewünschten Container.
3. Wählen Sie im Aktionsbereich des SafeGuard Management Center die Registerkarte **POA Gruppenzuweisung**.

   Unter **POA-Gruppen** auf der rechten Seite werden alle verfügbaren POA-Gruppen angezeigt.

4. Ziehen Sie die gewünschte POA-Gruppe aus **POA-Gruppen** in den **POA Gruppenzuweisung** Aktionsbereich.

   Gruppenname und **Gruppen-DSN** der POA-Gruppe werden im Aktionsbereich angezeigt.

5. Speichern Sie Ihre Änderungen in der Datenbank.

Alle Mitglieder der zugewiesenen POA-Gruppe werden an alle Endpoints im ausgewählten Container übertragen.

Sie können die Zuweisung aufheben oder die zugewiesene POA-Gruppe ändern, indem Sie wie beschrieben vorgehen und Gruppen von und in die Registerkarte **POA Gruppenzuweisung** und den Bereich **POA-Gruppen** ziehen.

Wenn Sie Ihre Änderungen in der Datenbank gespeichert haben, gilt die neue Zuweisung.

19.7.2 Zuweisen von POA-Benutzern zu Standalone-Endpoints

Um POA-Benutzer zu Standalone-Endpoints zuzuweisen, benötigen Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** für die relevante POA-Gruppe.

POA-Benutzer werden Standalone-Endpoints (im Standalone-Modus betrieben) in Konfigurationspaketen zugewiesen.

1. Wählen Sie im SafeGuard Management Center aus dem Menü **Extras** den Befehl **Konfigurationspakete**.
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.
3. Wählen Sie eine **POA-Gruppe** aus, die Sie zuvor im Bereich **Benutzer & Computer** des SafeGuard Management Center erstellt haben.

   Darüber hinaus steht standardmäßig eine **keine Liste** Gruppe zur Auswahl zur Verfügung. Diese Gruppe kann dazu verwendet werden, die Zuweisung einer POA-Gruppe auf Endpoints zu löschen.

4. Geben Sie einen Ausgabepfad für das Konfigurationspaket an.
5. Klicken Sie auf **Konfigurationspaket erstellen**.

6. Installieren Sie das Konfigurationspaket auf den Endpoints.

Durch Installation des Konfigurationspakets werden die Benutzer aus der Gruppe zur SafeGuard POA auf den Endpoints hinzugefügt. Die POA-Benutzer stehen für die Anmeldung an die POA zur Verfügung.

Hinweis: Wenn Sie Standalone-Endpoints auf zentral verwaltete Endpoints migrieren, bleiben die POA-Benutzer aktiv, wenn Sie auch im SafeGuard Management Center zugewiesen wurden. Die in den POA-Gruppen, die mit Konfigurationspaketen installiert wurden, gesetzten Kennwörter werden auf die im SafeGuard Management Center angegebenen Kennwörter gesetzt. Kennwörter, die mit **F8** geändert wurden, werden überschrieben. Weitere Informationen zur Migration von Standalone-Endpoints zu zentral verwalteten Endpoints finden Sie im *SafeGuard Enterprise upgrade guide*.

19.7.3 Aufheben der POA-Benutzer Zuweisung bei Standalone-Endpoints

POA-Benutzer lassen sich von Standalone-Endpoints entfernen, indem Sie eine leere POA-Gruppe zuweisen:

1. Wählen Sie im **Tools** Menü des SafeGuard Management Center den Befehl **Konfigurationspakete**.
2. Wählen Sie ein vorhandenes Konfigurationspaket aus oder erstellen Sie ein neues.
3. Wählen Sie eine leere **POA-Gruppe**, die Sie zuvor im Bereich **Benutzer & Computer** des SafeGuard Management Center angelegt haben, oder die **keine Liste** POA-Gruppe, die standardmäßig unter **Konfigurationspakete** zur Verfügung steht.
4. Geben Sie einen Ausgabepfad für das Konfigurationspaket an.
5. Klicken Sie auf **Konfigurationspaket erstellen**.
6. Installieren Sie das Konfigurationspaket auf den Endpoints.

Durch Installation des Konfigurationspakets werden alle POA-Benutzer von den Endpoints entfernt. Somit werden alle relevanten Benutzer aus der SafeGuard POA entfernt.

19.7.4 Ändern der POA-Benutzer Zuweisungen auf Standalone-Endpoints

1. Legen Sie eine neue POA-Gruppe an oder ändern Sie eine bestehende Gruppe.
2. Erstellen Sie ein neues Konfigurationspaket und wählen Sie die neue oder modifizierte POA-Gruppe aus.
3. Installieren Sie das Konfigurationspaket auf den Endpoints.

Die neue POA-Gruppe steht auf dem Endpoint zur Verfügung. Alle enthaltenen Benutzer werden zur POA hinzugefügt. Die neue Gruppe überschreibt die alte. POA-Gruppen werden nicht miteinander kombiniert.

19.8 Anmeldung an einem Endpoint mit einem POA-Benutzer

1. Schalten Sie den Endpoint ein.

   Der SafeGuard Power-on Authentication Anmeldedialog wird angezeigt.

2. Geben Sie den **Benutzernamen** und das **Kennwort** des vordefinierten POA-Benutzers ein.

   Sie werden nicht automatisch an Windows angemeldet. Der Windows-Anmeldedialog wird angezeigt.

3. Wählen Sie im **Domäne** Feld die Domäne **<POA>**.
4. Melden Sie sich mit Ihrem vorhandenen Windows-Benutzerkonto an Windows an.

19.8.1 Lokale Kennwortänderung

Wurde das Kennwort eines POA-Benutzers mit **F8**, geändert, so wird die Änderung nicht mit anderen Endpoints synchronisiert. Der Administrator muss das Kennwort für diesen Benutzer zentral ändern.

20 Richtlinieneinstellungen

SafeGuard Enterprise Richtlinien enthalten alle Einstellungen, die zur Abbildung einer unternehmensweiten Sicherheitsrichtlinie auf den Endpoints wirksam werden sollen.

In SafeGuard Enterprise Richtlinien können Sie Einstellungen für die folgenden Bereiche (Richtlinientypen) festlegen:

- **Allgemeine Einstellungen**

  Einstellungen für z. B. Transferrate, Anpassung, Recovery für die Anmeldung, Hintergrundbilder usw.

- **Authentisierung**

  Einstellungen zum Anmeldemodus, zur Gerätesperre usw.

- **PIN**

  Legt Anforderungen an die verwendeten PINs fest.

- **Kennwörter**

  Legt Anforderungen an die verwendeten Kennwörter fest.

- **Passphrasen**

  Legt Anforderungen für in SafeGuard Data Exchange verwendete Passphrasen fest.

- **Geräteschutz**

  Einstellungen für volume- oder dateibasierende Verschlüsselung (auch Einstellungen für SafeGuard Data Exchange, SafeGuard Cloud Storage und SafeGuard Portable): Algorithmen, Schlüssel, Laufwerke, auf denen Daten verschlüsselt werden sollen, usw.

- **Spezifische Computereinstellungen**

  Einstellungen zur SafeGuard Power-on Authentication (aktivieren/deaktivieren), zum sicheren Wake on LAN, Anzeigeoptionen usw.

- **Protokollierung**

  Legt fest, welche Ereignisse wo protokolliert werden.

- **Configuration Protection**

  Hinweis: Configuration Protection wird nur für SafeGuard Enterprise Clients bis zur Version 6,0 unterstützt. Dieser Richtlinientyp ist im 7.0 SafeGuard Management Center weiterhin für ältere Clients mit Configuration Protection enthalten.

  Einstellungen (erlauben/sperren) für die Verwendung von Ports, Peripheriegeräten (Wechselmedien, Druckern usw.)

- **Dateiverschlüsselung**

  Einstellungen für dateibasierende Verschlüsselung auf lokalen Festplatten und im Netzwerk, speziell für Arbeitsgruppen bei Netzwerkfreigaben.

Im SafeGuard Management Center stehen für alle Richtlinientypen Standardrichtlinien zur Verfügung. Für **Geräteschutz** Richtlinien stehen Richtlinien für die Festplattenverschlüsselung (Ziel: Massenspeicher), Cloud Storage (Ziel: DropBox) und Data Exchange (Ziel: Wechselmedien) zur Verfügung. Die Optionen in diesen Standardrichtlinien sind auf die relevanten Standardwerte gesetzt. Sie können die Standardeinstellungen Ihren Anforderungen anpassen. Die Standardrichtlinien haben den Namen <Richtlinientyp> (Default).

Hinweis: Die Namen der Standardrichtlinien richten sich nach der Spracheinstellung während der Installation. Wenn Sie die Sprache des SafeGuard Management Center nachträglich ändern, verbleiben die Namen der Standardrichtlinien in der während der Installation eingestellten Sprache.

20.1 Allgemeine Einstellungen

Richtlinieneinstellung	Erklärung
LADEN DER EINSTELLUNGEN	
Richtlinien-Loopback	**Computereinstellungen wiederholen** Wird unter **Richtlinien-Loopback** die Option **Computereinstellungen wiederholen** ausgewählt und die Richtlinie kommt von einem Computer (**Computereinstellungen wiederholen** einer Benutzer-Richtlinie hat keine Auswirkung), wird diese Richtlinie zum Schluss nochmals ausgeführt. Dadurch werden etwaige Benutzereinstellungen wieder überschrieben und es gelten die Computereinstellungen. **Benutzer ignorieren** Wird bei einer Richtlinie (Maschinen-Richtlinie) unter **Richtlinien-Loopback** die Einstellung **Benutzer ignorieren** ausgewählt und die Richtlinie "kommt" von einer Maschine, werden nur die Computereinstellungen ausgewertet. Benutzereinstellungen werden nicht ausgewertet. **Kein Loopback** **Kein Loopback** ist das Standardverhalten. Benutzerrichtlinien gelten vor Maschinenrichtlinien. **Wie werden die Einstellungen "Benutzer ignorieren" und "Computereinstellungen wiederholen" ausgewertet?** Existieren aktive Richtlinienzuweisungen, werden zuerst die Maschinenrichtlinien ausgewertet und vereinigt. Ergibt diese Vereinigung der einzelnen Richtlinien beim Richtlinien-Loopback den Wert **Benutzer ignorieren**, so werden Richtlinien, welche für den Benutzer bestimmt gewesen wären, nicht mehr ausgewertet. Das heißt sowohl für den Benutzer wie auch für die Maschine gelten die gleichen Richtlinien. Gilt nach der Vereinigung der einzelnen Maschinen-Richtlinien bei Richtlinien-Loopback der Wert **Computereinstellungen wiederholen**, werden die Benutzer-Richtlinien mit den Maschinen-Richtlinien vereinigt. Nach der Vereinigung werden die Maschinen-Richtlinien nochmals geschrieben und überschreiben gegebenenfalls Einstellungen aus Benutzer-Richtlinien. Das heißt: Ist eine Einstellung in beiden Richtlinien vorhanden, so ersetzt der

Richtlinieneinstellung	Erklärung
	Wert der Maschinen-Richtlinie den Wert der Benutzer-Richtlinie. Ergibt die Vereinigung der einzelnen Maschinen-Richtlinien "nicht konfiguriert", so gilt: Benutzereinstellungen vor Maschineneinstellungen.
TRANSFERRATE	
Server-Verbindungsintervall (in Minuten)	Legt den Zeitraum in Minuten fest, nach dem ein SafeGuard Enterprise Client beim SafeGuard Enterprise Server eine Anfrage nach Richtlinien (-änderungen) stellt. **Hinweis:** Um zu vermeiden, dass eine große Anzahl an Clients gleichzeitig den Server kontaktiert, findet die Kommunikation in einem Zeitraum +/- 50 % des eingestellten Intervalls statt. Beispiel: Wenn Sie "90 Minuten" einstellen, erfolgt die Kommunikation nach einem Intervall, das 45 bis 135 Minuten betragen kann.
PROTOKOLLIERUNG	
Rückmeldung nach Anzahl von Ereignissen	Das Protokollsystem, implementiert als Win32 Service "SGM LogPlayer", sammelt von SafeGuard Enterprise generierte, für die zentrale Datenbank bestimmte Protokolleinträge in lokalen Protokolldateien. Diese befinden sich im LocalCache im Verzeichnis "auditing\SGMTransLog ". Diese Dateien werden an den Transportmechanismus übergeben, der sie dann über den SGN Server in die Datenbank einträgt. Die Übertragung erfolgt sobald der Transportmechanismus eine Verbindung zum Server hergestellt hat. Die Protokolldatei wird daher größer, bis eine Verbindung hergestellt werden konnte. Um die Größe einer einzelnen Protokolldatei einschränken zu können, kann man über die Richtlinie eine maximale Anzahl von Protokolleinträgen eintragen. Dann wird die Protokolldatei vom Protokollsystem nach Erreichen der eingestellten Anzahl von Einträgen in die Transportqueue des SGN Servers gestellt und eine neue Protokolldatei begonnen
ANPASSUNG	
Sprache am Client	Legt fest, in welcher Sprache die Einstellungen für SafeGuard Enterprise auf dem Endpoint angezeigt werden. Sie können neben den unterstützten Sprachen kann auch die Betriebssystem-Spracheinstellung des Endpoint auswählen.
RECOVERY FÜR DIE ANMELDUNG	
Recovery für die Anmeldung nach Beschädigung des Windows Local Cache aktivieren	Der Windows Local Cache ist Start- und Endpunkt für den Datenaustausch zwischen Endpoint und Server. Im Windows Local Cache werden alle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien abgelegt. Alle im Local Cache gespeicherten Daten haben eine Signatur und können nicht manuell geändert werden.

Richtlinieneinstellung	Erklärung
	Standardmäßig ist der Recovery-Vorgang für die Anmeldung bei beschädigtem Local Cache deaktiviert. Er wird automatisch aus seiner Sicherungskopie wiederhergestellt. Für die Reparatur des Windows Local Cache ist also in diesem Fall kein Challenge/Response-Verfahren notwendig. Wenn der Windows Local Cache explizit über ein Challenge/Response-Verfahren repariert werden soll, wählen Sie in diesem Feld die Einstellung **Ja**.
Local Self Help	
Local Self Help aktivieren	Legt fest, ob sich Benutzer mit Local Self Help an ihrem Endpoint anmelden dürfen, wenn sie ihr Kennwort vergessen haben. Local Self Help ermöglicht Benutzern die Anmeldung durch die Beantwortung einer definierten Anzahl an zuvor festgelegten Fragen in der SafeGuard Power-on Authentication. Sie erhalten somit auch dann Zugriff zu ihrem Computer, wenn weder eine Internet- noch eine Telefonverbindung zur Verfügung stehen. **Hinweis:** Für die Benutzung von Local Self Help ist es notwendig, dass die automatische Anmeldung an Windows aktiviert ist. Andernfalls funktioniert die Anmeldung über Local Self Help nicht.
Minimale Länge der Antwort	Definiert die Mindestlänge in Zeichen für die Local Self Help Antworten.
Willkommenstext unter Windows	Hier können Sie einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten auf dem Endpoint im ersten Dialog angezeigt werden soll. Damit Sie den Text hier angeben können, muss dieser zunächst im **Richtliniennavigationsbereich** unter **Texte** angelegt werden.
Benutzer dürfen eigene Fragen festlegen	Die für Local Self Help zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an den Endpoint übertragen. Sie können die Benutzer jedoch auch per Richtlinie berechtigen, selbst Fragen zu definieren. Um die Benutzer zur Definition eigener Fragen zu berechtigen, wählen Sie in diesem Feld die Einstellung **Ja**.
Challenge / Response (C/R)	
Recovery für die Anmeldung über C/R aktivieren	Legt fest, ob ein Benutzer in der SafeGuard Power-on Authentication (POA) eine Challenge erzeugen darf, um über ein Challenge/Response-Verfahren wieder Zugang zu seinem Computer zu erhalten. **Ja**: Benutzer darf Challenge erzeugen. In diesem Fall kann der Benutzer über ein Challenge/Response-Verfahren in Notfällen wieder Zugang zu seinem Computer erlangen. **Nein**: Benutzer darf keine Challenge erzeugen. In diesem Fall kann der Benutzer im Notfall kein Challenge/Response-Verfahren starten, um wieder Zugang zu seinem Computer zu erlangen.

Richtlinieneinstellung	Erklärung
Automatische Anmeldung an Windows erlauben	Erlaubt dem Benutzer nach einer Authentisierung per Challenge/Response die automatische Anmeldung an Windows. **Ja**: Benutzer wird automatisch an Windows angemeldet. **Nein**: Windows-Anmeldebildschirm erscheint. **Beispiel**: Ein Benutzer hat sein Kennwort vergessen. SafeGuard Enterprise meldet ihn nach Austausch von Challenge und Response ohne SafeGuard Enterprise Kennwort am Endpoint an. In diesem Fall wird die automatische Anmeldung an Windows ausgeschaltet und der Windows-Anmeldebildschirm erscheint. Da der Benutzer sein SafeGuard Enterprise (= Windows-Kennwort) nicht weiß, kann er sich nicht anmelden. Mit **Ja** wird eine automatische Anmeldung erlaubt und der Benutzer bleibt nicht im Windows-Anmeldebildschirm stecken.
Texte	Zeigt nach dem Starten eines Challenge/Response-Vorgangs in der SafeGuard POA einen Informationstext. Zum Beispiel: “Bitte rufen Sie Ihren Support unter der Telefonnummer 01234-56789 an.”). Bevor Sie einen Text angeben können, muss dieser als Textdatei im **Richtlinien-Navigationsbereich** unter **Texte** erstellt werden.
BILDER	
	Voraussetzung: Neue Bilder müssen im SafeGuard Management Center im **Richtlinien-Navigationsbereich** unter **Bilder** registriert werden. Erst nach der Registrierung ist die Liste verfügbar. Unterstütztes Format: .BMP, PNG, JPEG.
Hintergrundbild in der POA **Hintergrundbild in der POA (niedrige Auflösung)**	Ersetzt das blaue SafeGuard Enterprise Hintergrundbild durch ein individuelles Hintergrundbild. Kunden können hier z. B. das Firmenlogo in der SafeGuard POA verwenden. Maximale Dateigröße für alle Hintergrundbilder: 500 KB Normal: ▪ Auflösung: 1024x768 (VESA-Modus) ▪ Farben: unbegrenzt Niedrig: ▪ Auflösung: 640 x 480 (VGA-Modus) ▪ Farben: 16 Farben
Anmeldebild in der POA **Anmeldebild in der POA (niedrige Auflösung)**	Ersetzt das während der SafeGuard POA-Anmeldung angezeigte SafeGuard Enterprise Bild durch ein individuelles Bild, z. B. das Firmenlogo. Normal:

Richtlinieneinstellung	Erklärung
	▪ Auflösung: 413 x 140 Pixel ▪ Farben: unbegrenzt Niedrig: ▪ Auflösung: 413 x 140 Pixel ▪ Farben: 16 Farben
Dateiverschlüsselung	
Vertrauenswürdige Anwendungen	Für die dateibasierende Verschlüsselung durch File Encryption und SafeGuard Data Exchange können Sie vertrauenswürdige Anwendungen angeben, die auf verschlüsselte Dateien zugreifen können. Dies ist zum Beispiel notwendig, damit Antivirus-Software verschlüsselte Dateien überprüfen kann. Geben Sie die Anwendungen, die Sie als vertrauenswürdig definieren möchten, in das Editor-Listenfeld des Felds ein. Anwendungen müssen als Fully Qualified Paths eingegeben werden.
Ignorierte Anwendungen	Für die dateibasierende Verschlüsselung durch File Encryption und SafeGuard Data Exchange können Sie ignorierte Anwendungen angeben, um Sie von der transparenten Dateiverschlüsselung/Dateientschlüsselung auszuschließen. Wenn Sie zum Beispiel ein Backup-Programm als ignorierte Anwendung definieren, bleiben die vom Programm gesicherten verschlüsselten Daten verschlüsselt. Geben Sie die Anwendungen, die Sie als ignoriert definieren möchten, in das Editor-Listenfeld des Felds ein. Anwendungen müssen als Fully Qualified Paths eingegeben werden.
Ignorierte Geräte	Für die dateibasierende Verschlüsselung durch File Encryption und SafeGuard Data Exchange können Sie ganze Geräte (zum Beispiel Festplatten) von der dateibasierende Verschlüsselung ausnehmen. Wählen Sie im Editor-Listenfeld **Netzwerk** aus, um ein vordefiniertes Gerät auszuwählen, oder geben Sie die erforderlichen Gerätenamen ein, um bestimmte Geräte von der Verschlüsselung auszuschließen.
Persistente Verschlüsselung aktivieren	Für die dateibasierende Verschlüsselung durch File Encryption und SafeGuard Data Exchange können Sie die persistente Verschlüsselung konfigurieren. Mit persistenter Verschlüsselung bleiben Kopien von verschlüsselten Dateien auch dann verschlüsselt, wenn sie an einem Speicherort abgelegt werden, für den keine Verschlüsselungsregel gilt. Diese Einstellung ist standardmäßig aktiviert.

Richtlinieneinstellung	Erklärung
Benutzer darf Standardschlüssel festlegen	Für die dateibasierende Verschlüsselung durch Cloud Storage können Sie festlegen, ob der Benutzer eine Standardschlüssel festlegen darf oder nicht. Wenn der Benutzer dies darf, steht der Befehl **Standardschlüssel festlegen** im Windows Explorer Kontextmenü der Cloud Storage Synchronisierungsordner zur Verfügung. Mit diesem Befehl können Benutzer separate Standardschlüssel angeben, die für die Verschlüsselung von unterschiedlichen Synchronisierungsordnern verwendet werden soll.

20.2 Authentisierung

Richtlinieneinstellung	Erklärung
ZUGRIFF	
Benutzer kann nur von interner Festplatte booten:	**Hinweis:** Diese Einstellung wird nur von Endpoints unterstützt, auf denen eine ältere SafeGuard Enterprise Version als 6.1 installiert ist. Mit dieser Option konnte es dem Benutzer ermöglicht werden, den Endpoint von externen Medien zu starten. Ab Version 6.1 hat diese Einstellung keine Wirkung mehr auf Endpoints. Für das betreffende Recovery-Szenario können Sie die Recovery mit virtuellen Clients verwenden (siehe Challenge/Response mit virtuellen Clients (Seite 245)). Legt fest, ob Benutzer den Computer von Festplatte und/oder anderem Medium starten dürfen. **JA**: Benutzer darf ausschließlich von der Festplatte booten. Die Möglichkeit, den Computer mit Diskette oder einem weiteren externen Medium zu starten, wird nicht in der SafeGuard POA angeboten. **NEIN**: Benutzer darf den Computer von Festplatte, Diskette oder einem externen Medium (USB, CD etc.) starten.
ANMELDEOPTIONEN	
Anmeldemodus	Legt fest, wie sich Benutzer in der SafeGuard POA authentisieren müssen. ▪ **Benutzername/Kennwort** Benutzer müssen sich mit ihrem Benutzernamen und Kennwort anmelden. ▪ **Token** Der Benutzer darf sich nur mit einem Token oder einer Smartcard in der SafeGuard POA anmelden. Dieses

Richtlinieneinstellung	Erklärung
	Verfahren bietet eine höhere Sicherheit. Bei der Anmeldung wird der Benutzer aufgefordert, seinen Token einzustecken. Durch den Besitz des Token und der Eingabe der PIN wird die Identität des Benutzers verifiziert. Nach korrekter Eingabe der PIN liest SafeGuard Enterprise automatisch die Daten für die Anmeldung des Benutzers aus. **Hinweis:** Beachten Sie, dass Sie sich bei Wahl dieses Anmeldeverfahrens nur mit einem vorher ausgestellten Token anmelden können. Die Einstellungen **Benutzername/Kennwort** und **Token** lassen sich kombinieren. Um zu prüfen, ob die Anmeldung mit Token reibungslos funktioniert, wählen Sie zunächst beide Einstellungen aus. Erst nach erfolgreicher Token-Anmeldung sollten Sie den Anmeldemodus **Benutzername/Kennwort** deaktivieren. Damit ein Umschalten zwischen den Anmeldemodi möglich ist, erlauben Sie den Benutzern, sich einmal mit beiden Einstellungen kombiniert anzumelden, da es sonst zu einer Blockierung bei der Anmeldung kommen kann. Wenn Sie Local Self Help für die Token-Anmeldung zulassen möchten, müssen Sie die beiden Einstellungen ebenfalls kombinieren. ▪ **Fingerabdruck** Wählen Sie diese Option, um die Anmeldung mit Lenovo-Fingerabdruck-Leser zu aktivieren. Benutzer, für die diese Richtlinie wirksam ist, können sich mit Fingerabdruck oder Benutzername/Kennwort anmelden. Dieser Vorgang bietet das höchste Maß an Sicherheit. Bei der Anmeldung führt die Benutzer den Finger über den Fingerabdruck-Leser. Wenn der Fingerabdruck erfolgreich erkannt wurde, liest die SafeGuard Power-on Authentication die Anmeldeinformationen des Benutzers und meldet den Benutzer an der Power-on Authentication an. Die Anmeldeinformationen werden dann an Windows übertragen und der Benutzer wird an seinem Computer angemeldet. **Hinweis:** Nach Auswahl dieses Anmeldevorgangs kann sich der Benutzer nur mit einem vorher registrierten Fingerabdruck oder mit Benutzername und Kennwort anmelden. Die Anmeldeverfahren Token und Fingerabdruck lassen sich auf einem Computer nicht miteinander kombinieren.
Anmeldeoptionen mit Token	Legt den Typ des Token bzw. der Smartcard fest, der am Endpoint verwendet werden soll. ▪ **Nicht kryptographisch**: Authentisierung bei der SafeGuard POA und bei Windows mittels Anmeldeinformationen. ▪ **Kerberos**: Zertifikatsbasierte Authentisierung an der SafeGuard POA und an Windows. Für zentral verwaltete Endpoints stellt der Sicherheitsbeauftragte ein Zertifikat in einer PKI aus und legt

Richtlinieneinstellung	Erklärung
	es auf dem Token ab. Dieses Zertifikat wird als Benutzerzertifikat in die SafeGuard Enterprise Datenbank importiert. Falls dort bereits ein automatisch erzeugtes Zertifikat existiert, wird es durch das importierte Zertifikat überschrieben. Kryptographische Token können nicht für Standalone-Endpoints verwendet werden. ▪ **Hinweis:** Bei Problemen bei der Anmeldung mit einem Kerberos-Token kann weder Challenge/Response noch Local Self Help für Recovery-Vorgänge benutzt werden. Hier wird nur Challenge/Response mit virtuellen Clients unterstützt. Mit diesem Verfahren können Benutzer wieder Zugriff auf verschlüsselte Volumes auf Ihren Endpoints erlangen.
PIN für automatische Anmeldung mit Token	Geben Sie hier eine Default-PIN an, die dem Benutzer die automatische Anmeldung an der SafeGuard Power-on Authentication mit Token oder Smartcard ermöglicht. Der Benutzer muss den Token bei der Anmeldung einstecken. Daraufhin wird eine automatische Anmeldung an der SafeGuard Power-on Authentication durchgeführt. Windows wird gestartet. PIN-Regeln müssen hier nicht beachtet werden. **Hinweis:** ▪ Diese Option steht nur dann zur Verfügung, wenn die Option **Token** als **Anmeldemodus** gewählt wurde. ▪ Wenn diese Option ausgewählt wird, muss bei **Durchgehende Anmeldung an Windows** die Einstellung **Durchgehende Anmeldung deaktivieren** gewählt werden.
Erfolglose Anmeldeversuche dieses Benutzers anzeigen	Wenn hier **Ja** eingestellt ist: Nach der Anmeldung bei SafeGuard POA und Windows wird ein Dialog mit Informationen über die letzte fehlgeschlagene Anmeldung (Benutzername/Datum/Zeit) angezeigt.
Letzte Benutzeranmeldung anzeigen	Wenn hier **Ja** eingestellt ist: Nach der Anmeldung bei SafeGuard POA und Windows wird ein Dialog mit folgenden Informationen angezeigt: ▪ Letzte erfolgreiche Anmeldung (Benutzername/Datum/Zeit) ▪ Letzte Anmeldeinformationen des angemeldeten Benutzers
'Erzwungene Abmeldung' bei Sperre der Arbeitsstation deaktivieren:	**Hinweis:** Diese Einstellung wird nur unter Windows XP wirksam. Windows XP wird mit SafeGuard Enterprise 6.1 nicht länger unterstützt. Die entsprechende Richtlinie ist im SafeGuard Management Center 7.0 noch verfügbar, um SafeGuard Enterprise 6 Clients zu unterstützen, die über ein 6.1 Management Center verwaltet werden.

Richtlinieneinstellung	Erklärung
	Wenn Benutzer den Endpoint nur für kurze Zeit verlassen wollen, können Sie den Rechner per Klick auf die Schaltfläche **Arbeitsstation sperren** für andere Benutzer sperren und danach mit ihrem Kennwort wieder entsperren. **Nein**: Sowohl der Benutzer, der die Arbeitsstation gesperrt hat, als auch ein Administrator kann die Sperre aufheben. Hebt ein Administrator die Sperre auf, so wird der aktuell angemeldete Benutzer zwangsweise abgemeldet. **Ja**: Diese Einstellung ändert dieses Verhalten. In diesem Fall kann nur der Benutzer die Sperre des Computers aufheben. Ein Aufheben der Sperre durch den Administrator und das damit verbundene erzwungene Abmelden des Benutzers ist nicht mehr möglich.
Letzte Benutzer/Domänen-Auswahl aktivieren	**Ja**: Die SafeGuard POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers. Benutzer müssen den Benutzernamen also nicht jedes Mal eingeben, wenn sie sich anmelden. **Nein**: Die SafeGuard POA speichert den Benutzernamen und die Domäne des letzten angemeldeten Benutzers nicht.
Service Account Liste	Um zu verhindern, dass durch administrative Vorgänge auf einem durch SafeGuard Enterprise geschützten Endpoint die Power-on Authentication aktiviert wird und Rollout-Beauftragte als Benutzer zum Endpoint hinzugefügt werden, bietet SafeGuard Enterprise Service Account Listen für die Windows-Anmeldung an SafeGuard Enterprise Endpoints. Die in den Listen enthaltenen Benutzer werden als SafeGuard Enterprise Gastbenutzer behandelt Damit Sie hier eine Liste auswählen können, müssen Sie diese zunächst im **Richtlinien**-Navigationsbereich unter **Service Account Listen** anlegen.
Durchgehende Anmeldung an Windows	**Hinweis:** Soll der Benutzer in der Lage sein, anderen Benutzern Zugriff auf “seinen“ Computer zu gewähren, muss er in der Lage sein, die durchgehende Anmeldung an Windows zu deaktivieren. ▪ **Benutzer wählen lassen** Im SafeGuard POA Anmeldedialog kann der Benutzer durch Aktivieren/Deaktivieren dieser Option entscheiden, ob er automatisch an Windows angemeldet werden will oder nicht. ▪ **Durchgehende Anmeldung deaktivieren** Nach der Anmeldung an der SafeGuard POA wird anschließend der Windows-Anmeldedialog angezeigt. Der Benutzer muss sich manuell an Windows anmelden. ▪ **Durchgehende Anmeldung erzwingen** Der Benutzer wird immer automatisch an Windows angemeldet.

Richtlinieneinstellung	Erklärung
BITLOCKER-OPTIONEN	
BitLocker Anmeldemodus für Boot-Laufwerke	Folgende Optionen stehen zur Verfügung: ▪ **TPM**: Der Schlüssel für die Anmeldung wird auf dem TPM-Chip (Trusted Platform Module) gespeichert. ▪ **TPM + PIN**: Der Schlüssel für die Anmeldung wird auf dem TPM-Chip gespeichert und zusätzlich wird eine PIN zur Anmeldung benötigt. ▪ **Systemstartschlüssel**: Der Schlüssel für die Anmeldung wird auf einem USB-Stick gespeichert. ▪ **TPM + Systemstartschlüssel**: Der Schlüssel für die Anmeldung wird auf dem TPM-Chip und auf einem USB-Stick gespeichert. Beides wird für die Anmeldung benötigt. **Hinweis:** Um die Anmeldemodi **TPM + PIN**, **TPM + Systemstartschlüssel** oder **Systemstartschlüssel** verwenden zu können, aktivieren Sie die Gruppenrichtlinie **Zusätzliche Authentifizierung beim Start anfordern** entweder im Active Directory oder auf den Computern lokal. Im lokalen Gruppenrichtlinien-Editor (**gpedit.msc**) sind die Gruppenrichtlinien hier zu finden: **Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drive** Um **Systemstartschlüssel** zu verwenden, müssen Sie auch **BitLocker ohne kompatibles TPM zulassen** in den Gruppenrichtlinien aktivieren. **Hinweis:** Wenn der momentan am System aktive Anmeldemodus ein erlaubter Fallback-Anmeldemodus ist, dann kommt der hier definierte Anmeldemodus nicht zur Anwendung.
BitLocker Anmeldemodus für Boot-Laufwerke - Fallback	Wenn die als **BitLocker Anmeldemodus für Boot-Laufwerke** festgelegte Einstellung nicht angewendet werden kann, bietet SafeGuard Enterprise folgende Alternativen für die Anmeldung: ▪ **Kennwort**: Der Benutzer muss ein Kennwort eingeben. ▪ **Systemstartschlüssel**: Der Schlüssel für die Anmeldung wird auf einem USB-Stick gespeichert. ▪ **Kennwort oder Systemstartschlüssel**: USB-Sticks werden nur verwendet, wenn Kennwörter auf dem Client-Betriebssystem nicht unterstützt werden. ▪ **Fehler**: Es wird eine Fehlermeldung angezeigt und das Volume wird nicht verschlüsselt. **Hinweis:** Bei Clients mit Version 6.1 oder niedriger werden die Werte **Kennwort oder Systemstartschlüssel** und **Kennwort** den alten Einstellungen **Systemstartschlüssel** und **Fehler** zugeordnet.

Richtlinieneinstellung	Erklärung
	Hinweis: Kennwörter werden erst ab Windows 8 oder höher unterstützt.
BitLocker Anmeldemodus für Datenlaufwerke	Bei Datenlaufwerken sind die folgenden Optionen verfügbar: ▪ **Auto-Unlock**: Wenn das Boot-Laufwerk verschlüsselt ist, wird ein externer Schlüssel generiert und auf dem Boot-Laufwerk gespeichert. Die Datenlaufwerke werden dann automatisch verschlüsselt. Sie werden automatisch mit der Auto-Unlock-Funktion von Bitlocker freigegeben. Beachten Sie, dass Auto-Unlock nur funktioniert, wenn das Boot-Laufwerk verschlüsselt ist. Andernfalls wird der Fallback-Modus verwendet. ▪ **Kennwort**: Der Benutzer wird aufgefordert, ein Kennwort für jedes Datenlaufwerk einzugeben. ▪ **Systemstartschlüssel**: Die Schlüssel für die Freigabe der Datenlaufwerke werden auf einem USB-Stick gespeichert. **Hinweis:** Clients mit Version 6.1 oder niedriger ignorieren diese Richtlinieneinstellung und verwenden stattdessen die Werte, die für den Anmeldemodus für Boot-Laufwerke eingestellt wurden. Da das TPM nicht für Datenlaufwerke genutzt werden kann, wird in diesen Fällen ein USB-Stick oder eine Fehlermeldung verwendet. **Hinweis:** Kennwörter werden erst ab Windows 8 oder höher unterstützt. **Hinweis:** Wenn der momentan am System aktive Anmeldemodus ein erlaubter Fallback-Anmeldemodus ist, dann kommt der hier definierte Anmeldemodus nicht zur Anwendung.
BitLocker Anmeldemodus für Datenlaufwerke - Fallback	Wenn die als **BitLocker Anmeldemodus für Datenlaufwerke** festgelegte Einstellung nicht angewendet werden kann, bietet SafeGuard Enterprise folgende Alternativen: ▪ **Kennwort**: Der Benutzer wird aufgefordert, ein Kennwort für jedes Datenlaufwerk einzugeben. ▪ **Systemstartschlüssel**: Die Schlüssel werden auf einem USB-Stick gespeichert. ▪ **Kennwort oder Systemstartschlüssel**: USB-Sticks werden nur verwendet, wenn Kennwörter auf dem Client-Betriebssystem nicht unterstützt werden. **Hinweis:** Clients mit Version 6.1 oder niedriger ignorieren diese Richtlinieneinstellung. Sie verwenden stattdessen die Werte, die für den Fallback-Anmeldemodus für Boot-Laufwerke eingestellt wurden. Da keine Kennwörter verarbeitet werden können, wird stattdessen "USB-Stick" oder "Fehlermeldung" verwendet. **Hinweis:** Kennwörter werden erst ab Windows 8 oder höher unterstützt.

Richtlinieneinstellung	Erklärung
ERFOLGLOSE ANMELDUNGEN	
Maximalanzahl von erfolglosen Anmeldeversuchen	Bestimmt, wie oft ein Benutzer ohne Folgen bei der Anmeldung einen ungültigen Benutzernamen bzw. ein ungültiges Kennwort eingeben darf. Wenn der Benutzer zum Beispiel drei mal nacheinander seinen Benutzernamen oder sein Kennwort falsch eingegeben hat, führt der vierte Versuch dazu, dass der Computer gesperrt wird.
Meldungen zur fehlgeschlagenen Anmeldung in der POA anzeigen	Definiert die Detailebene für Meldungen zu fehlgeschlagenen Anmeldungen: ▪ **Standard**: Zeigt eine kurze Beschreibung an. ▪ **Verbose** (ausführlich): Zeigt detaillierte Informationen an.
TOKEN-OPTIONEN	
Aktion bei Verlust des Anmeldestatus des Token	Definiert das Verhalten nach dem Trennen des Token vom Computer. Mögliche Aktionen sind: ▪ **Computer sperren** ▪ **PIN-Dialog anzeigen** ▪ **Keine Aktion**
Freigabe des Token erlauben	Bestimmt, ob der Token bei der Anmeldung entsperrt werden darf.
OPTIONEN FÜR SPERRE DES GERÄTS	
Bildschirm nach X Minuten Leerlauf sperren	Bestimmt die Zeit, nach deren Überschreitung ein nicht mehr benutzter Desktop automatisch gesperrt wird. Der Standardwert ist 0 Minuten, und der Bildschirm wird nicht gesperrt, wenn dieser Wert nicht geändert wird.
Bei Entfernung des Token Bildschirm sperren	Bestimmt, ob der Bildschirm gesperrt wird, wenn während einer Arbeitssitzung der Token entfernt wird.
Bildschirm nach dem Fortsetzen sperren	Bestimmt, ob der Bildschirm bei Reaktivierung aus dem Standby-Modus gesperrt wird.

20.3 Anlegen von Listen verbotener PINs für die Verwendung mit Richtlinien

Für Richtlinien des Typs **PIN** kann eine Liste mit verbotenen PINs angelegt werden. Diese Liste definiert die Zeichenfolgen, die in nicht in PINs verwendet werden dürfen. PINs werden für die Anmeldung mit Token verwendet. Weitere Informationen finden Sie unter Token und Smartcards (Seite 216).

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Textdateien beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien in einem anderen Format erstellen, werden sie bei der Registrierung automatisch in dieses Format konvertiert.

Hinweis: In den Listen werden die verbotenen PINs durch einen Zeilenumbruch voneinander getrennt.

So registrieren Sie die Textdateien:

1. Klicken Sie im Richtlinien-Navigationsbereich mit der rechten Maustaste auf **Texte** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.
3. Klicken Sie auf **[...]** um die zuvor erstellte Textdatei auszuwählen. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Texte** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich auf der rechten Seite angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

20.4 Syntaxregeln für PINs

In Richtlinien vom Typ **PIN** definieren Sie Einstellungen für Token-PINs. Diese Einstellungen gelten nicht für PINs, die zum Anmelden bei mit BitLocker verschlüsselten Endpoints verwendet werden. Weitere Informationen zu BitLocker PINs finden Sie unter PIN und Kennwörter (Seite 170).

PINs können sowohl Ziffern, Buchstaben als auch Sonderzeichen (wie + - ; etc.) enthalten. Verwenden Sie bei der Vergabe einer neuen PIN jedoch keine Zeichen mit der Kombination ALT + <Zeichen>, da dieser Eingabemodus an der SafeGuard Power-on Authentication nicht zur Verfügung steht.

Hinweis: Definieren Sie PIN-Regeln entweder im SafeGuard Management Center oder im Active Directory, nicht an beiden Stellen.

Richtlinieneinstellung	Erklärung
PIN	
Mindestlänge der PIN	Gibt an, aus wie vielen Zeichen eine PIN bei der Änderung durch den Benutzer bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungsschaltflächen vergrößert bzw. verkleinert werden.
Maximallänge der PIN	Gibt an, aus wie vielen Zeichen eine PIN bei der Änderung durch den Benutzer maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungsschaltflächen vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben **Mindestanzahl an Ziffern** **Mindestanzahl an Symbolen**	Mit diesen Einstellungen wird erreicht, dass PINs nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthalten, sondern aus einer Kombination bestehen müssen (z. B. „15blume“). Diese Einstellungen sind nur dann sinnvoll, wenn eine Mindestlänge der PIN definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird nur bei den Punkten **Liste nicht erlaubter PINs benutzen** und **Benutzername als PIN verboten** wirksam. **Beispiel 1:** Sie haben in der Liste der verbotenen PINs „Tafel“ eingetragen. Steht die Option **Groß-/Kleinschreibung beachten** auf **Ja**, werden zusätzliche Kennwortvarianten wie z. B. „TAFEL“ oder „TaFeL“ nicht akzeptiert und die Anmeldung wird verweigert. **Beispiel 2:** Der Benutzername für einen Anwender lautet „EMaier“. Steht **Groß-/Kleinschreibung beachten** auf **Ja** und **Benutzername als PIN verboten** auf **Nein**, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ usw.) als Kennwort verwenden.
Tastaturzeile verboten	Als Tastaturzeilen werden eingetippte Zeichenreihen wie „123“ oder „qwe“ bezeichnet. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „xsw2“ oder „3edc“ (nicht aber „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Kennwörter abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ▪ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“ oder „cba“). ▪ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als PIN verboten	Bestimmt, ob Benutzername und PIN identisch sein dürfen. **Ja**: Windows-Benutzername und PIN müssen unterschiedlich sein.

Richtlinieneinstellung	Erklärung
	Nein: Benutzer darf seinen Windows-Benutzernamen gleichzeitig als PIN verwenden.
Liste nicht erlaubter PINs benutzen	Bestimmt, ob bestimmte Zeichenfolgen für PINs nicht verwendet werden dürfen. Abgelegt sind die Zeichenfolgen in der **Liste nicht erlaubter PINs** (z. B. Datei im Format .txt).
Liste nicht erlaubter PINs	Definiert Zeichenfolgen, die in einer PIN nicht verwendet werden dürfen. Wenn ein Benutzer eine verbotene PIN verwendet, wird eine Fehlermeldung ausgegeben. **Voraussetzung:** Eine Liste (eine Datei) mit verbotenen PINs muss im Management Center unter **Texte** im Richtlinien-Navigationsbereich registriert werden. Erst nach der Registrierung ist die Liste verfügbar. Maximale Dateigröße: 50 KB Unterstütztes Format: Unicode **Nicht erlaubte PINs definieren** In der Liste werden die verbotenen PINs durch einen Zeilenumbruch voneinander getrennt. *Platzhalter:* An der Position, an der Sie den Zeichentyp „*“ eingeben, können mehrere beliebige Zeichen in der PIN enthalten sein. Beispielsweise wird durch *123* jede Zeichenfolge, die 123 enthält, als PIN verboten. **Hinweis:** ▪ Wenn Sie nur den Platzhalter in die Liste einfügen, können sich Benutzer nach einer erzwungenen Kennwortänderung nicht mehr im System anmelden. ▪ Benutzer dürfen auf die Datei keinen Zugriff haben. ▪ Die Option **Liste nicht erlaubter PINs verwenden** muss aktiviert sein.
ÄNDERUNGEN	
PIN-Änderung erlaubt nach mindestens (Tage)	Legt den Zeitraum fest, in dem eine PIN nicht erneut geändert werden darf. Diese Einstellung verhindert, dass ein Benutzer seine PIN innerhalb eines bestimmten Zeitraums beliebig oft ändern kann. **Beispiel:** Die Benutzerin Schmidt definiert eine neue PIN (z. B. „13jk56“). Für sie (oder für die Gruppe, der sie zugeordnet ist) ist ein Wechsel nach mind. fünf Tagen festgelegt. Bereits nach zwei Tagen will sie die PIN „13jk56“ ändern. Dies wird abgelehnt, da Frau Schmidt erst nach fünf Tagen eine neue PIN definieren darf.
PIN läuft ab nach (Tage)	Der Benutzer muss nach Ablauf des eingestellten Zeitraums seine PIN ändern. Beträgt der Zeitraum 999 Tage, ist keine PIN-Änderung erforderlich.

Richtlinieneinstellung	Erklärung
Warnung vor Ablauf (Tage)	Ab “n” Tagen vor Ablauf der PIN wird eine Warnmeldung ausgegeben und der Benutzer darauf hingewiesen, dass er in “n“-Tagen seine PIN ändern muss. Er erhält daraufhin die Möglichkeit, die PIN sofort zu ändern.
ALLGEMEIN	
PIN in POA verbergen	Gibt an, ob die Ziffern bei der Eingabe der PIN verborgen werden. Ist die Option aktiviert, wird während der Eingabe der PIN bei der POA nichts angezeigt. Ansonsten wird für jedes eingegebene Zeichen ein Stern angezeigt.
PIN-Generationen	Legt fest, wann bereits verwendete PINs wieder benutzt werden dürfen. Sinnvoll ist die Definition von PIN-Generationen insbesondere in Verbindung mit der Einstellung **PIN läuft ab nach (Tage)**. **Beispiel:** Die Anzahl der PIN-Generationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer die PIN wechseln muss, auf 30. Herr Müller meldete sich bislang mit der PIN „Informatik“ an. Nach Ablauf der Frist von 30Tagen wird er aufgefordert, seine PIN zu ändern. Herr Müller tippt als neue PIN wieder „Informatik“ ein und erhält die Fehlermeldung, dass er diese PIN bereits verwendet hat und eine andere PIN wählen muss. „Informatik“ darf Herr Müller erst nach der vierten (da PIN-Generationen = 4) Aufforderung zur Eingabe einer neuen PIN verwenden.

20.5 Anlegen einer Liste verbotener Kennwörter für die Verwendung mit Richtlinien

Für Richtlinien des Typs **Kennwort** kann eine Liste mit verbotenen Kennwörtern angelegt werden. Diese Liste definiert die Zeichenfolgen, die in nicht in Kennwörtern verwendet werden dürfen.

Hinweis: In den Listen werden die nicht erlaubten Kennwörter durch einen Zeilenumbruch voneinander getrennt.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Textdateien beträgt **50 KB**. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien in einem anderen Format erstellen, werden sie bei der Registrierung automatisch in dieses Format konvertiert.

Wenn eine Datei konvertiert wird, wird eine entsprechende Meldung angezeigt.

So registrieren Sie die Textdateien:

1. Klicken Sie im Richtlinien-Navigationsbereich mit der rechten Maustaste auf **Texte** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.

3. Klicken Sie auf **[...]** um die zuvor erstellte Textdatei auszuwählen. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Texte** im Richtlinien-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich auf der rechten Seite angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

Hinweis: Mit der Schaltfläche **Text ändern** können Sie weiteren Text zum bestehenden Text hinzufügen. Es wird ein Dialog geöffnet, in dem eine weitere Textdatei ausgewählt werden kann. Der in dieser Datei enthaltene Text wird am Ende des bestehenden Texts eingefügt.

20.6 Syntaxregeln für Kennwörter

In Richtlinien vom Typ **Kennwort** definieren Sie Einstellungen für Kennwörter für die Anmeldung an das System. Diese Einstellungen gelten nicht für Kennwörter, die zum Anmelden bei mit BitLocker verschlüsselten Endpoints verwendet werden. Weitere Informationen zu BitLocker-Kennwörtern finden Sie unter PIN und Kennwörter (Seite 170).

Kennwörter können sowohl Ziffern, Buchstaben als auch Sonderzeichen (wie + - ; etc.) enthalten. Verwenden Sie bei der Vergabe eines neuen Kennworts jedoch keine Zeichen mit der Kombination ALT + <Zeichen>, da dieser Eingabemodus an der SafeGuard Power-on Authentication nicht zur Verfügung steht. Wie Kennwörter, mit denen sich Benutzer am System anmelden, beschaffen sein müssen, wird in Richtlinien vom Typ **Kennwort** eingestellt.

Hinweis: Informationen zur Umsetzung einer Richtlinie für sichere Kennwörter finden Sie unter Empfohlene Sicherheitsmaßnahmen (Seite 11) sowie im *SafeGuard Enterprise Manual for certification-compliant operation* (Englisch).

Die Umsetzung von Kennwortregeln und Kennworthistorien kann nur dann gewährleistet werden, wenn der SGN Credential Provider durchgehend verwendet wird. Definieren Sie Kennwortregeln entweder im SafeGuard Management Center oder im Active Directory, nicht an beiden Stellen.

Richtlinieneinstellung	Erklärung
KENNWORT	
Mindestlänge des Kennworts	Gibt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungsschaltflächen vergrößert bzw. verkleinert werden.
Maximallänge des Kennwortes	Gibt an, aus wie vielen Zeichen ein Kennwort bei der Änderung durch den Benutzer maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungsschaltflächen vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben **Mindestanzahl an Ziffern**	Mit diesen Einstellungen wird erreicht, dass Kennwörter nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthalten, sondern aus einer Kombination bestehen müssen (z. B.

Richtlinieneinstellung	Erklärung
Mindestanzahl an Symbolen	„15blume“). Diese Einstellungen sind nur dann sinnvoll, wenn eine Kennwortmindestlänge definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird nur bei den Punkten **Liste nicht erlaubter Kennwörter verwenden** und **Benutzername als Kennwort verboten** wirksam. **Beispiel 1:** Sie haben in der Liste der verbotenen Kennwörter „Tafel“ eingetragen. Steht die Option **Groß-/Kleinschreibung beachten** auf **Ja**, werden zusätzliche Kennwortvarianten wie z. B. „TAFEL“ oder „TaFeL“ nicht akzeptiert und die Anmeldung wird verweigert. **Beispiel 2:** Der Benutzername für einen Anwender lautet „EMaier“. Steht **Groß-/Kleinschreibung beachten** auf **Ja** und **Benutzername als Kennwort verboten** auf **Nein**, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ usw.) als Kennwort verwenden.
Tastaturzeile verboten	Als Tastaturzeilen werden eingetippte Zeichenreihen wie „123“ oder „qwe“ bezeichnet. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „xsw2“ oder „3edc“ (nicht aber „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Kennwörter abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ▪ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“ oder „cba“). ▪ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als Kennwort verboten	Legt fest, dass der Benutzername nicht als Kennwort verwendet werden darf. **Ja**: Windows-Benutzername und Kennwort müssen unterschiedlich sein. **Nein**: Windows-Benutzername und Kennwort müssen nicht unterschiedlich sein.
Liste nicht erlaubter Kennwörter verwenden	Bestimmt, ob bestimmte Zeichenfolgen für Kennwörter nicht verwendet werden dürfen. Abgelegt sind die Zeichenfolgen in der **Liste nicht erlaubter Kennwörter** (z. B. Datei im Format .txt).

Richtlinieneinstellung	Erklärung
Liste nicht erlaubter Kennwörter	Definiert Zeichenfolgen, die in einem Kennwort ausgeschlossen sind. Wenn ein Benutzer ein verbotenes Kennwort verwendet, wird eine Fehlermeldung ausgegeben. Eine Liste (eine Datei) mit verbotenen Kennwörtern muss im SafeGuard Management Center unter **Texte** im Richtlinien-Navigationsbereich registriert werden. Erst nach der Registrierung ist die Liste verfügbar. Maximale Dateigröße: 50 KB Unterstütztes Format: Unicode **Nicht erlaubte Kennwörter definieren** In der Liste werden die verbotenen Kennwörter durch einen neuen Zeilenanfang getrennt. *Platzhalter:* An der Position, an der Sie den Zeichentyp "*" eingeben, können mehrere beliebige Zeichen im Kennwort enthalten sein. Beispielsweise wird durch *123* jede Zeichenfolge, die 123 enthält, als Kennwort verboten. **Hinweis:** ▪ Wenn Sie nur den Platzhalter in die Liste einfügen, können sich Benutzer nach einer erzwungenen Kennwortänderung nicht mehr im System anmelden. ▪ Benutzer dürfen auf die Datei keinen Zugriff haben. ▪ Die Option **Liste nicht erlaubter Kennwörter verwenden** muss aktiviert sein.
Benutzerkennwortsynchronisation mit anderen SGN Clients	Dieses Feld steuert die Synchronisierung bei Änderung des Kennworts durch Benutzer, die auf mehreren SafeGuard Enterprise Endpoints arbeiten und als Benutzer eingetragen sind. Folgende Optionen stehen zur Verfügung: ▪ Langsam (sobald Benutzer sich anmeldet) Ändert ein Benutzer sein Kennwort auf einem SafeGuard Enterprise Endpoint, so muss dieser Benutzer sich auf anderen Endpoints, auf denen er als Benutzer eingetragen ist, zunächst noch einmal mit seinem alten Kennwort an der SafeGuard Power-on Authentication anmelden. Erst dann wird die Kennwortsynchronisation durchgeführt ▪ Schnell (sobald der Computer eine Verbindung hergestellt hat) Ändert der Benutzer sein Kennwort auf einem SafeGuard Enterprise Endpoint, so wird die Kennwortsynchronisierung mit einem anderen Endpoint, auf dem er als Benutzer eingetragen ist, durchgeführt, sobald der andere Endpoint eine Verbindung mit dem Server hergestellt hat. Dies erfolgt zum Beispiel dann, wenn sich ein anderer Benutzer, der ebenfalls auf dem Endpoint als Benutzer eingetragen ist, in der Zwischenzeit an diesem Endpoint anmeldet.
ÄNDERUNGEN	

Richtlinieneinstellung	Erklärung
Kennwortänderung erlaubt nach mindestens (Tage)	Legt den Zeitraum fest, in dem ein Kennwort nicht erneut geändert werden darf. Diese Einstellung verhindert, dass ein Benutzer sein Kennwort innerhalb eines bestimmten Zeitraums beliebig oft ändern kann. Bei einem durch Windows erzwungenen Kennwortwechsel oder bei einem Wechsel des Kennworts nach der Anzeige der Warnung, dass das Kennwort in x Tagen abläuft, wird diese Einstellung nicht ausgewertet! **Beispiel:** Die Benutzerin Schmidt definiert ein neues Kennwort (z. B. „13jk56"). Für sie (oder für die Gruppe, der sie zugeordnet ist) ist ein Wechsel nach mind. fünf Tagen festgelegt. Bereits nach zwei Tagen will sie das Kennwort "13jk56" ändern. Dies wird abgelehnt, da Frau Schmidt erst nach fünf Tagen ein neues Kennwort definieren darf.
Kennwort läuft ab nach (Tage)	Ist diese Option aktiviert, muss der Benutzer nach Ablauf des eingestellten Zeitraums ein neues Kennwort definieren.
Warnung vor Ablauf (Tage)	Ab "n" Tagen vor Ablauf des Kennworts wird eine Warnmeldung ausgegeben und der Benutzer darauf hingewiesen, dass er in "n" Tagen sein Kennwort ändern muss. Er erhält daraufhin die Möglichkeit, das Kennwort sofort zu ändern.
ALLGEMEIN	
Kennwort in POA verbergen	Gibt an, ob die Zeichen bei der Eingabe des Kennworts verborgen werden. Ist die Option aktiviert, wird während der Eingabe des Kennworts bei der POA nichts angezeigt. Ansonsten wird für jedes eingegebene Zeichen ein Stern angezeigt.
Kennwortgenerationen	Legt fest, wann bereits verwendete Kennwörter wieder benutzt werden dürfen. Sinnvoll ist die Definition von Kennwortgenerationen insbesondere in Verbindung mit der Einstellung **Kennwort läuft ab nach (Tage)**. **Beispiel:** Die Anzahl der Kennwortgenerationen für den Benutzer Müller wurde auf 4 festgelegt, die der Tage, nach denen der Benutzer das Kennwort wechseln muss, auf 30. Herr Müller meldete sich bislang mit dem Kennwort „Informatik" an. Nach Ablauf der Frist von 30 Tagen wird er aufgefordert, sein Kennwort zu ändern. Herr Müller tippt als neues Kennwort wieder „Informatik" ein und erhält die Fehlermeldung, dass er dieses Kennwort bereits verwendet hat und ein anderes Kennwort wählen muss. „Informatik" darf Herr Müller erst nach der vierten (da Kennwortgenerationen = 4) Aufforderung zur Eingabe eines neuen Kennworts verwenden. **Hinweis:** Wenn für die Kennwortgeneration 0 eingestellt ist, kann der Benutzer das alte Kennwort als neues Kennwort festlegen. Dies entspricht jedoch nicht der gängigen Praxis und ist daher nicht zu empfehlen.

20.7 Passphrase für SafeGuard Data Exchange

Der Benutzer muss eine Passphrase eingeben, die zum Erzeugen von lokalen Schlüsseln für den sicheren Datenaustausch mit SafeGuard Data Exchange verwendet wird. Die auf den Endpoints erzeugten Schlüssel werden auch in der SafeGuard Enterprise Datenbank gespeichert. Die erforderlichen Einstellungen definieren Sie in einer Richtlinie vom Typ **Passphrase**.

Weitere Informationen zu SafeGuard Data Exchange finden Sie unter SafeGuard Data Exchange (Seite 193).

Weitere Informationen zu SafeGuard Data Exchange und SafeGuard Portable auf dem Endpoint finden Sie in der *SafeGuard Enterprise Benutzerhilfe* im Kapitel *SafeGuard Data Exchange*.

Richtlinieneinstellung	Erklärung
PASSPHRASE	
Mindestlänge der Passphrase	Legt fest, aus wie vielen Zeichen die Passphrase, aus der der Schlüssel erzeugt wird, mindestens bestehen muss. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Maximallänge der Passphrase	Legt fest, aus wie vielen Zeichen die Passphrase maximal bestehen darf. Der gewünschte Wert kann entweder direkt eingegeben oder durch Betätigen der Richtungstasten vergrößert bzw. verkleinert werden.
Mindestanzahl an Buchstaben **Mindestanzahl an Ziffern** **Mindestanzahl an Symbolen**	Mit diesen Einstellungen wird erreicht, dass eine Passphrase nicht ausschließlich Zeichen, Ziffern oder Sonderzeichen enthält, sondern aus einer Kombination bestehen muss (z. B. „15blume“). Diese Einstellungen sind nur dann sinnvoll, wenn eine Mindestlänge der PIN definiert ist, die größer 2 ist.
Groß-/Kleinschreibung beachten	Diese Einstellung wird beim Setzen der Option **Benutzername als Passphrase verboten** wirksam. **Beispiel:** Der Benutzername für einen Anwender lautet „EMaier“. Steht **Groß-/Kleinschreibung beachten** auf Ja und **Benutzername als Passphrase verboten** auf Nein, darf Benutzer EMaier keine Variante seines Benutzernamens (z. B. ´emaier´ oder ´eMaiEr´ etc.) als Passphrase verwenden.
Tastaturzeile verboten	Als Tastaturzeilen werden eingetippte Zeichenreihen wie „123“ oder „qwe“ bezeichnet. Maximal zwei auf der Tastatur nebeneinander liegende Zeichen sind erlaubt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.
Tastaturspalte verboten	Als Tastaturspalten werden eingetippte Zeichenreihen wie „xsw2“ oder „3edc“ (nicht aber „xdr5“ oder „cft6“!) bezeichnet. Erlaubt sind maximal zwei in einer Tastaturspalte befindliche Zeichen. Verbieten Sie Tastaturspalten, werden derartige Zeichenkombinationen als Passphrase abgelehnt. Tastaturspalten beziehen sich nur auf den alphanumerischen Tastaturteil.

Richtlinieneinstellung	Erklärung
Drei oder mehr aufeinanderfolgende Zeichen verboten	Verboten werden mit Aktivierung dieser Option Zeichenketten, ▪ die im ASCII-Code aufeinander folgen, sowohl in auf- als auch in absteigender Reihenfolge („abc“ oder „cba“). ▪ die aus drei oder mehr identischen Zeichen („aaa“ oder „111“) bestehen.
Benutzername als Passphrase verboten	Bestimmt, ob Benutzername und Passphrase identisch sein dürfen. **Ja**: Windows-Benutzername und Passphrase müssen unterschiedlich sein. **Nein**: Benutzer darf seinen Windows-Benutzernamen gleichzeitig als Passphrase verwenden.

20.8 White Lists für Geräteschutz-Richtlinien für dateibasierende Verschlüsselung

Im SafeGuard Management Center können Sie White Lists als Ziele für Richtlinien des Typs **Geräteschutz** für dateibasierende Verschlüsselung auswählen. Somit können Sie Verschlüsselungsrichtlinien für spezifische Gerätemodelle und sogar für spezifische Geräte erstellen.

Damit Sie eine White List als Ziel für eine **Geräteschutz** Richtlinie auswählen können, müssen Sie die Liste im SafeGuard Management Center anlegen. Sie können White Lists für spezifische Gerätemodelle (z. B. iPod, USB-Geräte eines bestimmten Herstellers usw.) oder für einzelne Geräte nach Seriennummer definieren. Sie können die Geräte manuell zu den White Lists hinzufügen oder die Ergebnisse eines SafeGuard Port Auditor Scan-Vorgangs verwenden. Weitere Informationen finden Sie im *SafeGuard PortAuditor User Guide*.

Sie können dann die White List als Ziel beim Anlegen einer Richtlinie vom Typ **Geräteschutz** auswählen.

Hinweis: Wenn Sie eine White List für eine Richtlinie vom Typ **Geräteschutz** als Ziel auswählen, können Sie als **Verschlüsselungsmodus für Medien** nur **Keine Verschlüsselung** oder **Dateibasierend** auswählen. Wenn Sie **Keine Verschlüsselung** für eine **Geräteschutz** Richtlinie mit einer White List auswählen, wird durch diese Richtlinie ein Gerät dann nicht von der Verschlüsselung ausgenommen, wenn eine andere geltende Richtlinie die volume-basierende Verschlüsselung fordert.

Hinweis: Für Block Master SafeStick gelten spezielle Anforderungen. Diese Geräte haben für Administratoren und Benutzer ohne Administratorrechte unterschiedliche IDs. Für die korrekte Verarbeitung in SafeGuard Enterprise müssen Sie beide IDs zur White List hinzufügen. Der SafeGuard Port Auditor ermittelt beide IDs, wenn ein SafeStick-Gerät mindestens einmal auf dem von SafeGuard Port Auditor gescannten Computer geöffnet wurde.

20.8.1 Anlegen einer White List für Geräteschutz-Richtlinien für die dateibasierende Verschlüsselung

1. Markieren Sie im **Richtlinien** Navigationsbereich den Eintrag **White List**.

2. Klicken Sie im Kontextmenü von **White List** auf **Neu > White List**.
3. Wählen Sie den Typ der White List aus:
   - Um eine White List für spezifische Datenträgermodelle zu erstellen, wählen Sie **Datenträgermodelle**.
   - Um eine White List für bestimmte Datenträger nach Seriennummer zu erstellen, wählen Sie **Einzelne Datenträger**.
4. Geben Sie unter **White List-Quelle** an, wie Sie die White List erstellen möchten:
   - Um Datenträger manuell einzugeben, wählen Sie **White List manuell erstellen**.

     Wenn Sie auf **OK** klicken, wird eine leere White List im SafeGuard Management Center geöffnet. In dieser leeren White List können Sie die Einträge manuell erstellen. Klicken Sie dazu auf das grüne Symbol **Hinzufügen (Einfügen)** in der SafeGuard Management Center Symbolleiste.

     Hinweis: Um die relevanten Strings für ein Gerät mit dem Windows-Geräte-Manager abzurufen, öffnen Sie das **Eigenschaften** Fenster für das Gerät und entnehmen Sie die Werte für die Eigenschaften **Hardware-Kennungen** und **Geräteinstanzkennung**. Es werden nur folgende Schnittstellen unterstützt: USB, 1394, PCMCIA und PCI.
   - Wenn Sie das Ergebnis eines Endpoint Scans durch den SafeGuard Port Auditor als Quelle verwenden möchten, wählen Sie **SafeGuard Port Auditor Ergebnis importieren**.

     Die Ergebnisse des Scans durch den SafeGuard Port Auditor müssen vorliegen (XML-Datei), wenn Sie die White List auf diese Weise erzeugen wollen. Um die Datei auszuwählen, klicken Sie auf die **[...]** Schaltfläche.

     Weitere Informationen hierzu finden Sie in der *SafeGuard PortAuditor Benutzerhilfe.*

     Nach dem Klicken auf **OK** wird der Inhalt der importierten Datei im SafeGuard Management Center angezeigt.

Die White List wird unter **White Lists** im **Richtlinien** Navigationsbereich angezeigt. Sie können Sie beim Erstellen von Richtlinien des Typs **Geräteschutz** für dateibasierende Verschlüsselung auswählen.

20.8.2 Auswahl einer White List als Ziel für Geräteschutz-Richtlinien für die dateibasierende Verschlüsselung

Voraussetzung: Die gewünschte White List muss im SafeGuard Management Center angelegt sein.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf die Schaltfläche **Richtlinien**.
2. Klicken Sie im Navigationsfenster mit der rechten Maustaste auf **Richtlinien** und wählen Sie im Kontextmenü den Befehl **Neu**.
3. Wählen Sie **Geräteschutz**.

   Es wird ein Dialog für die Benennung der neuen Richtlinie angezeigt.
4. Geben Sie einen Namen und optional eine Beschreibung für die neue Richtlinie ein.
5. Wählen Sie unter **Ziel des Geräteschutzes** die relevante White List:
   - Wenn Sie eine White List für Datenträgermodelle erstellt haben, wird sie unter **Datenträgermodelle** angezeigt.

- Wenn Sie eine White List für bestimmte Datenträger erstellt haben, wird sie unter **Einzelne Datenträger** angezeigt.

6. Klicken Sie auf **OK**.

Die White List ist als Ziel der Richtlinie vom Typ **Geräteschutz** ausgewählt. Nach der Übertragung der Richtlinie an die Endpoints gilt der in der Richtlinie festgelegte Verschlüsselungsmodus.

20.9 Geräteschutz

Richtlinien des Typs **Geräteschutz** enthalten Einstellungen für die Datenverschlüsselungen auf unterschiedlichen Datenträgern. Die Verschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen. Richtlinien des Typs **Geräteschutz** enthalten auch Einstellungen für SafeGuard Data Exchange, SafeGuard Cloud Storage und SafeGuard Portable. Weitere Informationen zu SafeGuard Data Exchange finden Sie unter SafeGuard Data Exchange (Seite 193). Weitere Informationen zu SafeGuard Cloud Storage finden Sie unter Cloud Storage (Seite 203). Weitere Informationen zu SafeGuard Data Exchange, SafeGuard Cloud Storage und SafeGuard Portable auf dem Endpoint finden Sie in der *SafeGuard Enterprise Benutzerhilfe*.

Wenn Sie eine Richtlinie dieses Typs erstellen, müssen Sie zunächst ein Ziel für den Geräteschutz angeben. Mögliche Ziele sind:

- Massenspeicher (Boot-Laufwerke/Andere Volumes)
- Wechselmedien
- Optische Laufwerke
- Datenträgermodelle
- Einzelne Datenträger
- Cloud Storage Definitionen

Für jedes Ziel muss eine eigene Richtlinie angelegt werden.

Hinweis: Ziel Wechselmedien: Eine Richtlinie für die volume-basierende Verschlüsselung von Wechsellaufwerken, die es dem Benutzer erlaubt, einen Schlüssel aus einer Liste auszuwählen (z. B. **Beliebiger Schlüssel im Schlüsselring des Benutzers**), kann vom Benutzer umgangen werden, indem er keinen Schlüssel auswählt. Um sicherzustellen, dass Wechsellaufwerke immer verschlüsselt werden, verwenden Sie eine dateibasierende Verschlüsselungsrichtlinie legen Sie in der volume-basierenden Verschlüsselungsrichtlinie explizit einen Schlüssel fest.

Richtlinieneinstellung	Erklärung
Verschlüsselungsmodus für Medien	Dient dem Schutz von Endgeräten (PCs, Notebooks usw.) und allen Arten von Wechseldatenträgern. **Hinweis:** Diese Einstellung ist obligatorisch. Hauptaufgabe ist die Verschlüsselung aller auf lokalen oder externen Datenträgern gespeicherten Daten. Durch die transparente Arbeitsweise können Benutzer einfach ihre gewohnten Anwendungen, z. B. Microsoft Office, weiter benutzen. Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten

Richtlinieneinstellung	Erklärung
	Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird diese automatisch wieder verschlüsselt. Folgende Optionen stehen zur Verfügung: ▪ **Keine Verschlüsselung** ▪ **Volume-basierend**(= transparente, sektorbasierende Verschlüsselung) Stellt sicher, dass alle Daten verschlüsselt sind (inkl. Boot-Dateien, Swapfile, Datei für den Ruhezustand/Hibernation File, temporäre Dateien, Verzeichnisinformationen usw.) ohne dass sich der Benutzer in seiner Arbeitsweise anpassen oder auf Sicherheit achten muss. ▪ **Dateibasierend** (= transparente, dateibasierte Verschlüsselung, Smart MediaEncryption) Stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen), mit dem Vorteil, dass auch optische Medien wie CD/DVD verschlüsselt werden können oder Daten mit Fremdrechnern, auf denen kein SafeGuard Enterprise installiert ist, ausgetauscht werden können (soweit von der Richtlinie erlaubt). **Hinweis:** Für Richtlinien mit White Lists können nur die Optionen **Keine Verschlüsselung** oder **Dateibasierend** ausgewählt werden.
ALLGEMEINE EINSTELLUNGEN	
Algorithmus für die Verschlüsselung	Setzt den Verschlüsselungsalgorithmus. Liste aller einsetzbaren Algorithmen mit ihren jeweiligen Standards: AES256: 32 Bytes (256 Bits) AES128: 16 Bytes (128 Bits)
Schlüssel für die Verschlüsselung	Legt fest, welcher Schlüssel zur Verschlüsselung verwendet wird. Es können bestimmte Schlüssel festgelegt werden (z. B. Computer-Schlüssel, oder ein definierter Schlüssel) oder dem Benutzer kann die Auswahl eines Schlüssels erlaubt werden. Die Schlüssel, die ein Benutzer verwenden darf, können eingeschränkt werden. Folgende Optionen stehen zur Verfügung: ▪ **Beliebiger Schlüssel im Schlüsselring des Benutzers** Alle Schlüssel aus dem Schlüsselbund des Benutzers werden angezeigt und der Benutzer darf einen daraus auswählen. **Hinweis:** Diese Option muss gewählt werden, wenn eine Richtlinie für dateibasierende Verschlüsselung für einen durch SafeGuard Enterprise geschützten Standalone-Endpoint angelegt wird. ▪ **Alle, außer persönliche Schlüssel im Schlüsselring**

<table>
<tr><th>Richtlinieneinstellung</th><th>Erklärung</th></tr>
<tr><td></td><td>Alle Schlüssel aus dem Schlüsselbund mit Ausnahme des persönlichen Schlüssels werden angezeigt und der Benutzer darf einen daraus auswählen.

▪ Beliebiger Gruppenschlüssel im Schlüsselring des Benutzers
Alle Gruppenschlüssel aus dem Schlüsselbund des Benutzers werden angezeigt und der Benutzer darf einen daraus auswählen.

▪ Definierter Computerschlüssel
Es wird der Maschinen-Schlüssel verwendet - der Benutzer selbst kann KEINEN Schlüssel auswählen.
Hinweis: Diese Option muss gewählt werden, wenn eine Richtlinie für volume-basierende Verschlüsselung für einen durch SafeGuard Enterprise geschützten Standalone-Endpoint angelegt wird. Wenn Sie dennoch die Option Beliebiger Schlüssel im Schlüsselring des Benutzers auswählen und der Benutzer wählt einen lokal erzeugten Schlüssel für die volume-basierende Verschlüsselung, wird der Zugriff auf dieses Volume verweigert.

▪ Beliebiger Schlüssel im Schlüsselring des Benutzers außer lokal erzeugte Schlüssel
Alle Schlüssel aus dem Schlüsselring mit Ausnahme der lokal erzeugten Schlüsse werden angezeigt und der Benutzer darf einen daraus auswählen

▪ Definierter Schlüssel aus der Liste
Der Administrator kann in der Administration bei der Richtlinien-Einstellung einen beliebigen, existierenden Schlüssel auswählen.</td></tr>
<tr><td></td><td>Der Schlüssel muss unter Für Verschlüsselung definierter Schlüssel ausgewählt werden.
Bei Verwendung von „Definierter Computer-Schlüssel“
Ist SafeGuard Enterprise Device Encryption nicht auf einem Endpoint installiert (keine SafeGuard POA, keine volume-basierende Verschlüsselung), wird eine Richtlinie, die den Definierten Computerschlüssel als Schlüssel für die dateibasierende Verschlüsselung festlegt, nicht auf dem Endpoint wirksam. Der definierte Computerschlüssel ist auf einem Endpoint dieses Typs nicht verfügbar. Die Daten können nicht verschlüsselt werden.
Richtlinien für durch SafeGuard Enterprise geschützte Standalone-Endpoints:
Hinweis: Bitte beachten Sie beim Erstellen von Richtlinien für Standalone-Computer, dass für die dateibasierende Verschlüsselung ausschließlich die Option Beliebiger Schlüssel im Schlüsselring des Benutzers möglich ist. Zusätzlich darf das Erzeugen von lokalen Schlüsseln nicht verboten werden.
Falls die Medien-Passphrase-Funktion für Unmanaged Endpoints aktiviert ist, wird der Medienverschlüsselungsschlüssel automatisch</td></tr>
</table>

Richtlinieneinstellung	Erklärung
	als **Für Verschlüsselung definierter Schlüssel** verwendet, da auf Unmanaged Endpoints keine Gruppenschlüssel zur Verfügung stehen. Wenn Sie beim Erstellen einer Wechselmedien-Richtlinie für Standalone-Endpoints einen anderen Schlüssel unter **Für Verschlüsselung definierter Schlüssel** auswählen, so hat dies keine Auswirkung.
Für Verschlüsselung definierter Schlüssel	Dieses Feld wird nur dann aktiv, wenn Sie im Feld **Schlüssel für die Verschlüsselung** die Option **Definierter Schlüssel aus der Liste** ausgewählt haben. Klicken Sie auf die Schaltfläche **[...]**, um den Dialog **Schlüssel suchen** aufzurufen. Klicken Sie auf **Jetzt suchen**, um nach Schlüsseln zu suchen und wählen Sie einen Schlüssel aus der angezeigten Liste aus. Bei einer Richtlinie vom Typ **Geräteschutz** mit dem Ziel **Wechselmedien** wird dieser Schlüssel zur Verschlüsselung des Medienverschlüsselungsschlüssel verwendet, wenn die Medien-Passphrase-Funktionalität aktiviert ist (**Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** auf **Ja** eingestellt). Für Richtlinien vom Typ **Geräteschutz** für Wechselmedien müssen daher die Einstellungen ▪ **Schlüssel für die Verschlüsselung** ▪ **Für Verschlüsselung definierter Schlüssel** unabhängig voneinander spezifiziert werden. **Richtlinien für durch SafeGuard Enterprise geschützte Standalone-Endpoints:** Falls die Medien-Passphrase-Funktion für Unmanaged Endpoints aktiviert ist, wird der Medienverschlüsselungsschlüssel automatisch als **Für Verschlüsselung definierter Schlüssel** verwendet, da auf Unmanaged Endpoints keine Gruppenschlüssel zur Verfügung stehen.
Benutzer darf einen lokalen Schlüssel erzeugen	Diese Einstellung bestimmt, ob Benutzer auf ihren Computern lokale Schlüssel erzeugen dürfen oder nicht. Lokale Schlüssel werden auf dem Endpoint basierend auf einer vom Benutzer eingegebenen Passphrase erzeugt. Die Anforderungen, denen eine Passphrase entsprechen muss, können in Richtlinien vom Typ **Passphrase** festgelegt werden. Diese Schlüssel werden ebenfalls in der Datenbank gespeichert. Der Benutzer kann sie auf jedem Endpoint, auf dem er sich anmelden darf, verwenden. Lokale Schlüssel können zum sicheren Datenaustausch über SafeGuard Data Exchange (SG DX) verwendet werden.
VOLUME-BASIERENDE EINSTELLUNGEN	
Benutzer darf dem verschlüsseltem Volume	**Ja**: Endpoint-Benutzer dürfen einen zusätzlichen Schlüssel aus einem Schlüsselbund einfügen/entfernen. Der Dialog wird angezeigt

Richtlinieneinstellung	Erklärung
Schlüssel hinzufügen oder diese entfernen	über den Kontextmenüeintrag **Eigenschaften/Verschlüsselung** / Registerkarte. **Nein**: Endpoint-Benutzer dürfen keine zusätzlichen Schlüssel hinzufügen.
Reaktion auf unverschlüsselte Volumes	Definiert, wie SafeGuard Enterprise mit unverschlüsselten Medien umgeht: Folgende Optionen stehen zur Verfügung: ▪ **Abweisen** (= Klartext-Medium wird nicht verschlüsselt) ▪ **Nur unverschlüsselte Medien akzeptieren und verschlüsseln** ▪ **Alle Medien akzeptieren und verschlüsseln**
Benutzer darf Volume entschlüsseln	Bewirkt, dass der Benutzer über einen Kontextmenü-Eintrag im Windows Explorer das Laufwerk entschlüsseln darf.
Schnelle Initialverschlüsselung	Wählen Sie diese Einstellung aus, um den Modus der schnellen Initialverschlüsselung für die volume-basierende Verschlüsselung zu aktivieren. Dieser Modus reduziert den Zeitraum, der für die Initialverschlüsselung auf Endpoints benötigt wird. **Hinweis:** Dieser Modus kann zu einem unsicheren Zustand führen. For further information, see Schnelle Initialverschlüsselung (Seite 167).
Bei defekten Sektoren fortfahren	Legt fest, ob die Verschlüsselung fortgesetzt oder gestoppt werden soll, wenn defekte Sektoren entdeckt werden. Die Standardeinstellung ist **Ja**.
DATEIBASIERENDE EINSTELLUNGEN	
Initialverschlüsselung aller Dateien	Bewirkt, dass die Initialverschlüsselung für ein Laufwerk automatisch nach der Benutzeranmeldung gestartet wird. Der Benutzer muss eventuell vorher einen Schlüssel aus dem Schlüsselbund auswählen.
Benutzer darf Initialverschlüsselung abbrechen	Bewirkt, dass der Benutzer die Initialverschlüsselung abbrechen kann.
Benutzer darf auf unverschlüsselte Dateien zugreifen	Definiert, ob ein Benutzer auf unverschlüsselte Dateien auf einem Laufwerk zugreifen darf.
Benutzer darf Dateien entschlüsseln	Bewirkt, dass der Benutzer einzelne Dateien oder ganze Verzeichnisse entschlüsseln kann (über die Windows Explorer-Erweiterung <rechte Maustaste>).

Richtlinieneinstellung	Erklärung
Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen	Bewirkt, dass der Benutzer eine Medien-Passphrase auf seinem Endpoint festlegen kann. Die Medien-Passphrase ermöglicht den einfachen Zugriff auf alle lokalen Schlüssel auf Computern ohne SafeGuard Data Exchange über SafeGuard Portable.
Nur für Wechselmedien und Cloud Storage: **SafeGuard Portable auf das Ziel kopieren**	Wenn diese Option ausgewählt ist, wird SafeGuard Portable auf alle Wechselmedien, die mit dem Endpoint verbunden werden, sowie in alle Synchronisierungsordner, die in einer Cloud Storage Definition für SafeGuard Cloud Storage definiert sind, kopiert. SafeGuard Portable ermöglicht den verschlüsselten Datenaustausch mit Wechselmedien oder Cloud Storage, ohne dass der Empfänger der Daten SafeGuard Enterprise installiert haben muss. Der Empfänger kann mit Hilfe von SafeGuard Portable und der entsprechenden Passphrase die verschlüsselten Daten entschlüsseln und auch wieder verschlüsseln. Der Empfänger kann mit SafeGuard Portable die Daten neu verschlüsseln oder den ursprünglich verwendeten Schlüssel für die Verschlüsselung verwenden. SafeGuard Portable muss nicht auf den Computer des Empfängers installiert oder kopiert werden, sondern kann direkt von den Wechselmedien oder von Cloud Storage aus verwendet werden.
Standardschlüssel für die Initialverschlüsselung	Über einen Dialog kann ein Schlüssel ausgewählt werden, der für die dateibasierte Initialverschlüsselung verwendet wird. Der Benutzer kann dann beim Start der Initialverschlüsselung keinen Schlüssel wählen. Die Initialverschlüsselung startet ohne Benutzerinteraktion. Für die Initialverschlüsselung wird immer der hier festgelegte Schlüssel verwendet. **Beispiel:** **Voraussetzung:** Ein Standardschlüssel für die Initialverschlüsselung ist gesetzt. Verbindet der Benutzer ein USB-Gerät mit dem Computer, startet die Initialverschlüsselung automatisch. Der definierte Schlüssel wird benutzt. Es ist kein Benutzereingriff notwendig. Will der Benutzer anschließend Dateien umschlüsseln oder neue Dateien auf dem USB-Medium speichern, kann er einen beliebigen Schlüssel auswählen (falls erlaubt und verfügbar). Schließt er dann ein anderes USB-Gerät an, wird wiederum der Schlüssel, der für die Initialverschlüsselung festgelegt wurde, zur Initialverschlüsselung verwendet. Dieser Schlüssel wird auch für folgende Verschlüsselungsoperationen verwendet, bis der Benutzer explizit einen anderen Schlüssel auswählt. **Hinweis:** Wenn die Medien-Passphrase-Funktion aktiviert ist, wird diese Option deaktiviert. Der **Für Verschlüsselung definierte Schlüssel** wird verwendet.
Klartext-Ordner	Der hier angegebene Ordner wird auf allen Wechselmedien, Massenspeichern und in allen Cloud Storage Synchronisierungsordnern erstellt. Dateien, die in diesen Ordner kopiert werden, bleiben immer unverschlüsselt.

Richtlinieneinstellung	Erklärung
Benutzer darf über Verschlüsselung entscheiden	Sie können den Benutzer dazu berechtigen zu entscheiden, ob Dateien auf Wechselmedien und Massenspeichern verschlüsselt werden sollen: ▪ Wenn Sie hier **Ja** auswählen, werden Benutzer dazu aufgefordert zu entscheiden, ob Daten verschlüsselt werden sollen. Für Massenspeicher wird diese Aufforderung nach jeder Anmeldung angezeigt. Für Wechselmedien wird sie angezeigt, wenn die Wechselmedien mit dem Computer verbunden werden. ▪ Wenn Sie für diese Option **Ja, Benutzereinstellungen merken** auswählen, können die Benutzer die Option **Einstellungen speichern und Dialog nicht mehr anzeigen** wählen, um ihre Auswahl für das relevante Gerät zu speichern. In diesem Fall wird der Dialog für das Gerät nicht mehr angezeigt. Wenn der Benutzer im auf dem Endpoint angezeigten Dialog **Nein** wählt, wird weder eine initiale noch eine transparente Verschlüsselung durchgeführt.

20.10 Spezifische Computereinstellungen - Grundeinstellungen

Richtlinieneinstellungen	Erklärung
POWER-ON AUTHENTICATION (POA)	
Power-on Authentication aktivieren	Definiert, ob die SafeGuard POA ein- oder ausgeschaltet sein soll. **Wichtig:** Aus Sicherheitsgründen empfehlen wir dringend, die SafeGuard POA eingeschaltet zu lassen. Durch Deaktivierung der SafeGuard POA reduziert sich die Systemsicherheit auf den Schutz durch die Windows-Anmeldung. Dadurch erhöht sich das Risiko des unberechtigten Zugriffs auf verschlüsselte Daten.
Zugriff verweigern, falls keine Verbindung zum Server in Tagen (0= keine Überprüfung)	Verweigert eine Anmeldung in der SafeGuard POA, wenn zwischen Endpoint und Server länger als festgelegt keine Verbindung bestand.
SICHERES WAKE ON LAN (WOL)	Mit den **Sicheres Wake On LAN** Einstellungen können Sie Endpoints für Software Rollouts vorbereiten. Nach dem Wirksamwerden einer solchen Richtlinie auf Endpoints werden die notwendigen Parameter (z. B. SafeGuard POA-Deaktivierung und ein Zeitabstand für Wake

Richtlinieneinstellungen	Erklärung
	on LAN) direkt an die Endpoints übertragen, wo sie analysiert werden. **Wichtig:** Wir weisen an dieser Stelle ausdrücklich darauf hin, dass auch das zeitlich begrenzte "Ausschalten" der SafeGuard POA für eine bestimmte Anzahl von Boot-Vorgängen ein Absenken des Sicherheitsniveaus bedeutet. Weitere Informationen zu sicherem Wake on LAN finden Sie unter Sicheres Wake on LAN (WOL) (Seite 232).
Anzahl der automatischen Anmeldungen	Definiert die Anzahl der Neustarts mit ausgeschalteter SafeGuard Power-on Authentication für Wake on LAN. Diese Einstellung überschreibt temporär die Einstellung von **Power-on Authentication aktivieren**, bis die Anzahl der eingestellten automatischen Anmeldungen erreicht ist. Danach wird die SafeGuard Power-on Authentication wieder aktiviert. Wenn Sie die Anzahl an automatischen Anmeldungen auf zwei einstellen und **Power-on Authentication aktivieren** aktiv ist, startet der Endpoint zweimal ohne Authentisierung durch die SafeGuard POA. Wir empfehlen, für Wake on LAN immer **drei Neustarts mehr als notwendig für Wartungsarbeiten** zu erlauben, um unvorhergesehene Probleme zu umgehen.
Lokale Windows-Anmeldung während WOL erlauben	Bestimmt, ob lokale Windows-Anmeldungen während Wake on LAN erlaubt sind.
Beginn des Zeitfensters für externen WOL Start **Ende des Zeitfensters für externen WOL Start**	Datum und Uhrzeit für den Beginn und das Ende des Wake on LAN (WOL) können ausgewählt oder eingegeben werden. Datumsformat: *MM/DD/YYYY* Uhrzeitformat: *HH:MM* Folgende Eingabekombinationen sind möglich: ▪ Beginn und Ende des WOL werden festgelegt. ▪ Nur das Ende des WOL wird festgelegt, der Beginn bleibt offen. ▪ Keine Einträge: Es wird kein Zeitintervall für den Client festgelegt Bei einem geplanten Software Rollout sollte der Sicherheitsbeauftragte den Zeitrahmen für WOL so bemessen, dass das Scheduling-Skript früh

Richtlinieneinstellungen	Erklärung
	genug startet und allen Endpoints genügend Zeit zum Booten bleibt. WOLstart: Der Startpunkt für den WOL im Scheduling-Skript muss innerhalb des hier in der Richtlinie festgelegten Zeitintervalls liegen. Wenn kein Intervall definiert ist, wird WOL lokal am durch SafeGuard Enterprise geschützten Endpoint nicht aktiviert. WOLstop: Dieses Kommando wird unabhängig vom hier festgelegten Endpunkt des WOL ausgeführt.
BENUTZER-COMPUTER ZUORDNUNG (UMA)	
SGN Gastbenutzer nicht zulassen	**Hinweis:** Diese Einstellung gilt nur für zentral verwaltete Endpoints. Legt fest, ob sich Gastbenutzer am Endpoint anmelden können. **Hinweis:** Microsoft Konten werden immer als SafeGuard Enterprise Gastbenutzer behandelt.
Registrieren von neuen SGN-Benutzern erlauben	Gibt an, wer einen anderen SGN-Benutzer in die SafeGuard POA und/oder UMA importieren kann (indem die durchgehende Anmeldung an das Betriebssystem deaktiviert wird). **Hinweis:** Bei Endpoints, auf denen das Device Encryption-Modul nicht installiert ist, muss die Einstellung **Registrieren von neuen SGN-Benutzern erlauben** auf **Jeder** gesetzt sein, wenn es auf dem Endpoint möglich sein soll, der UMA mehrere Benutzer hinzuzufügen, die Zugriff auf ihre Schlüsselringe haben sollen. Sonst können Benutzer nur im Management Center hinzugefügt werden. Diese Option ist wird nur auf zentral verwalteten Endpoints ausgewertet. Siehe auch Neue SafeGuard Enterprise Data Exchange-Benutzer erhalten nach dem Anmelden bei SafeGuard Enterprise Data Exchange Only Clients kein Zertifikat.
Registrierung von SGN Windows-Benutzern aktivieren	Legt fest, ob SGN Windows-Benutzer auf dem Endpoint registriert werden können. Ein SGN Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er auf verschlüsselte Dateien zugreifen kann wie ein SGN-Benutzer. Wenn Sie diese Einstellung wählen, werden alle Benutzer, die andernfalls SGN-Gast-Benutzer geworden wären, zu SGN Windows-Benutzern.

Richtlinieneinstellungen	Erklärung
	Die Benutzer werden zur UMA hinzugefügt, sobald sie sich an Windows angemeldet haben.
Manuelle UMA Bereinigung für Standalone Clients aktivieren	**Hinweis:** Diese Einstellung gilt nur für Standalone-Endpoints. Legt fest, ob Benutzer SGN-Benutzer und SGN Windows-Benutzer aus der Benutzer-Computer Zuordnung entfernen dürfen. Wenn Sie hier **Ja** auswählen, steht der Befehl **Benutzer-Computer Zuordnung** im System Tray Icon Menü auf dem Endpoint zur Verfügung. Mit diesem Befehl wird eine Liste von Benutzern angezeigt, die sich bei der SafeGuard Power-on Authentication als SGN-Benutzer und bei Windows als SGN Windows-Benutzer anmelden können. Im angezeigten Dialog können Benutzer aus der Liste entfernt werden. Nach dem Entfernen von SGN-Benutzern oder SGN Windows-Benutzern, können sich diese nicht mehr an der SafeGuard Power-on Authentication oder an Windows anmelden.
Maximale Anzahl von SGN Windows - Benutzern bevor Benutzer automatisch gelöscht werden	**Hinweis:** Diese Einstellung gilt nur für zentral verwaltete Endpoints. Mit dieser Einstellung können Sie eine automatisch Bereinigung der SafeGuard Enterprise Windows-Benutzer auf zentral verwalteten Endpoints aktiviert. Sobald der hier gesetzte Schwellwert von einem SafeGuard Enterprise Windows-Benutzer überschritten wird, werden alle vorhandenen SafeGuard Enterprise Windows-Benutzer außer dem neuen aus der Benutzer-Computer Zuordnung entfernt. Die Standardeinstellung ist **10**.
ANZEIGEOPTIONEN	
Computer-Identifikation anzeigen	Zeigt in der Titelleiste der SafeGuard POA entweder den Computernamen oder einen frei definierbaren Text an. Existiert ein Computername in den Windows-Netzwerkeinstellungen, wird dieser in der Grundeinstellung automatisch übernommen.
Text für Computer-Identifikation	Der Text, der in der Titelleiste der SafeGuard POA angezeigt werden soll. Ist unter **Computer-Identifikation anzeigen** die Option **Definierter Name** ausgewählt, können Sie in diesem Eingabefeld den Text eingeben.

Richtlinieneinstellungen	Erklärung
Rechtliche Hinweise anzeigen	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die vor der Anmeldung in der SafeGuard POA erscheint. In manchen Ländern ist das Erscheinen eines Textfelds mit bestimmtem Inhalt gesetzlich vorgeschrieben. Die Box muss vom Benutzer bestätigt werden, bevor das System fortfährt. Bevor Sie einen Text angeben können, muss dieser als Textelement im **Richtlinien** Navigationsbereich unter **Texte** registriert werden.
Text für rechtliche Hinweise	Text, der als rechtlicher Hinweis angezeigt werden soll. Sie können hier ein Textelement auswählen, das im **Richtlinien** Navigationsbereich unter **Texte** registriert wurde.
Zusätzliche Informationen anzeigen	Zeigt eine Textbox mit frei konfigurierbarem Inhalt an, die nach den rechtlichen Hinweisen (wenn diese aktiviert sind) erscheint. Sie können festlegen, ob die zusätzlichen Informationen angezeigt werden: ▪ Nie ▪ Bei jedem Systemstart ▪ Bei jeder Anmeldung Bevor Sie einen Text angeben können, muss dieser als Textelement im **Richtlinien** Navigationsbereich unter **Texte** registriert werden.
Text für zusätzliche Informationen	Text, der als zusätzliche Information angezeigt werden soll. Sie können hier ein Textelement auswählen, das im **Richtlinien** Navigationsbereich unter **Texte** registriert wurde.
Anzeigedauer (in Sekunden)	Zeitraum (in Sekunden) für die Anzeige zusätzlicher Informationen. Sie können hier die Anzahl der Sekunden eingeben, nach denen die Textbox für zusätzliche Informationen automatisch geschlossen wird. Der Benutzer kann die Textbox jederzeit durch Klicken auf **OK** schließen.
System Tray Icon aktivieren und anzeigen	Über das SafeGuard Enterprise System Tray Icon kann auf dem Endpoint einfach und schnell auf

Richtlinieneinstellungen	Erklärung
	alle Benutzerfunktionen zugegriffen werden. Zusätzlich können für den Benutzer Informationen über den Status des Endpoint (neue Richtlinien erhalten usw.) über Balloon Tool Tips ausgegeben werden. **Ja:** System Tray Icon wird im Infobereich der Taskleiste angezeigt, der Benutzer wird über Balloon Tool Tips laufend über den Status des durch SafeGuard Enterprise geschützten Endpoint. **Nein:** System Tray Icon wird nicht angezeigt. Keine Statusinformationen für den Benutzer über Ballon Tool Tips. **Stumm:** System Tray Icon wird im Infobereich der Taskleiste angezeigt, es werden aber keine Statusinformationen für den Benutzer über Ballon Tool Tips ausgegeben.
Overlay-Symbole im Explorer anzeigen	Bestimmt, ob im Windows Explorer Schlüsselsymbole zur Anzeige des Verschlüsselungsstatus von Volumes, Geräten, Ordnern und Dateien angezeigt werden.
Virtuelle Tastatur in der POA	Bestimmt, ob im SafeGuard POA-Anmeldedialog bei Bedarf eine virtuelle Tastatur zur Eingabe des Kennworts angezeigt werden kann.
INSTALLATIONSOPTIONEN	
Deinstallation erlaubt	Bestimmt, ob die Deinstallation von SafeGuard Enterprise auf den Endpoints möglich ist. Wird **Deinstallation erlaubt** auf **Nein** gesetzt, kann SafeGuard Enterprise solange eine Richtlinie mit dieser Einstellung wirksam ist, auch mit Administratorrechten nicht deinstalliert werden.
Sophos Manipulationsschutz aktivieren	Aktiviert/deaktiviert die Funktion Sophos Manipulationsschutz. Wenn Sie die Deinstallation von SafeGuard Enterprise über die Richtlinieneinstellung **Deinstallation erlaubt** als zulässig definiert haben, können Sie diese Richtlinieneinstellung auf **Ja** setzen, um Deinstallationsvorgänge durch die Funktion Sophos Manipulationsschutz überprüfen zu lassen und somit ein leichtfertiges Entfernen der Software zu verhindern.

Richtlinieneinstellungen	Erklärung
	Erlaubt die Funktion Sophos Manipulationsschutz die Deinstallation nicht, wird der Deinstallationsvorgang abgebrochen. Ist **Sophos Manipulationsschutz aktivieren** auf **Nein** eingestellt, werden SafeGuard Enterprise Deinstallationsvorgänge durch die Funktion Sophos Manipulationsschutz weder geprüft noch verhindert. **Hinweis:** Diese Einstellung gilt nur für Endpoints, auf denen Sophos Endpoint Security and Control in der Version 9.5 oder einer neueren Version installiert ist.
EINSTELLUNGEN FÜR CREDENTIAL PROVIDERS	
Credential Provider Wrapping	In SafeGuard Enterprise können Sie konfigurieren, dass ein anderer Credential Provider als der Windows Credential Provider verwendet wird. Vorlagen für die unterstützten Credential Provider stehen auf Sophos.com zum Download zur Verfügung. Eine Liste mit Vorlage für getestete Credential Provider sowie die Information zum Download erhalten Sie vom Sophos Support. Mit Hilfe der Richtlinieneinstellung **Credential Provider** können Sie eine Vorlage importieren und auf Endpoints anwenden. Klicken Sie auf **Vorlage importieren** und suchen Sie nach der Vorlagendatei. Die importierte Vorlage und deren Inhalt werden im mehrzeiligen Feld **Credential Provider**angezeigt und als Richtlinie eingestellt. Um eine Vorlage zu löschen, klicken Sie auf **Vorlage löschen**. **Hinweis:** Bearbeiten Sie die bereitgestellten Vorlagendateien nicht. Wenn die XML-Struktur dieser Dateien geändert wird, werden die Einstellungen unter Umständen auf dem Endpoint nicht erkannt. Dann wird unter Umständen der Standard Windows Credential Provider verwendet.
EINSTELLUNGEN FÜR DIE TOKENUNTERSTÜTZUNG	
Token Middleware Modulname	Registriert das PKCS#11 Modul eines Token. Folgende Optionen stehen zur Verfügung: ▪ ActivIdentity ActivClient ▪ ActivIdentity ActivClient (PIV) ▪ AET SafeSign Identity Client ▪ Aladdin eToken PKI Client

<table>
<tr><th>Richtlinieneinstellungen</th><th>Erklärung</th></tr>
<tr><td></td><td>

a.sign Client
ATOS CardOS API
Charismathics Smart Security Interface
Estonian ID-Card
Gemalto Access Client
Gemalto Classic Client
Gemalto .NET Card
IT Solution trustware CSP+
Módulo PKCS#11 TC-FNMT
Nexus Personal
RSA Authentication Client 2.x
RSA Smart Card Middleware 3.x
Siemens CardOS API
T-Systems NetKey 3.0
Unizeto proCertum
Benutzerdefinierte PKCS#11 Einstellungen...
Wenn Sie Benutzerdefinierte PKCS#11 Einstellungen... auswählen, werden die Benutzerdefinierten PKCS#11 Einstellungen aktiviert.
Sie können dann die zu verwendenden Modulnamen eingeben:

PKCS#11 Modul für Windows
PKCS#11 Modul für die SafeGuard Power-on Authentication (POA)

Hinweis: Wenn Sie Nexus Personal oder Gemalto .NET Card Middleware installieren, müssen Sie den Installationspfad der Middleware auch zur PATH-Umgebungsvariable der Systemeigenschaften Ihres Computers hinzufügen.

Standard-Installationspfad für Gemalto .NET Card: <code>C:\Programme\ Gemalto\PKCS11 for .NET V2 smart cards</code>
Standard-Installationspfad für Nexus Personal: <code>C:\Programme\Personal\bin</code>

Lizenzen:
</td></tr>
</table>

Richtlinieneinstellungen	Erklärung
	Beachten Sie, dass für die Benutzung der jeweiligen Middleware für das Standard-Betriebssystem eine Lizenzvereinbarung mit dem jeweiligen Hersteller erforderlich ist. Informationen darüber, wo Sie die Lizenzen erhalten, finden Sie unter Beschaffung der erforderlichen Middleware-Lizenzen für das Betriebssystem gemäß den Voraussetzungen von SafeGuard Device Encryption. Wenn Sie Siemens-Lizenzen erwerben möchten, wenden Sie sich an: Atos IT Solutions and Services GmbH Otto-Hahn-Ring 6 D-81739 München Germany
Dienste, auf die gewartet wird	Diese Einstellung dient zur Problembehebung mit bestimmten Token. Entsprechende Einstellungen werden gegebenenfalls von unserem Support bekannt gegeben.

20.11 Protokollierung bei Windows Endpoints

Ereignisse für SafeGuard Enterprise können in der Windows-Ereignisanzeige oder in der SafeGuard Enterprise Datenbank protokolliert werden. Um festzulegen, welche Ereignisse an welchem Ziel protokolliert werden sollen, erstellen Sie eine Richtlinie vom Typ **Protokollierung** und wählen Sie die gewünschten Ereignisse per Mausklick aus.

Es steht eine Vielzahl von Ereignissen aus unterschiedlichen Kategorien (z. B. Anmeldung, Verschlüsselung usw.) zur Auswahl zur Verfügung. Es ist daher empfehlenswert, eine Vorgehensweise für die Protokollierung zu definieren und die notwendigen Ereignisse unter Berücksichtigung der Anforderungen für Berichte und Audits festzulegen.

Weitere Informationen finden Sie unter Berichte (Seite 270).

21 Festplattenverschlüsselung

Diese Version von SafeGuard Enterprise unterstützt Windows 7 und Windows 8 auf Endpoints mit BIOS oder UEFI.

- Für Systeme mit BIOS können Sie zwischen SafeGuard Enterprise Festplattenverschlüsselung und von SafeGuard Enterprise verwalteter BitLocker Verschlüsselung wählen. Die BIOS Version verwendet den BitLocker-eigenen Wiederherstellungsmechanismus.

  Hinweis: Wenn in diesem Handbuch von SafeGuard Power-on Authentication oder SafeGuard Festplattenverschlüsselung die Rede ist, dann bezieht sich das nur auf Windows 7 BIOS Endpoints.

- Für UEFI Systeme verwenden Sie die von SafeGuard Enterprise verwaltete BitLocker Verschlüsselung für die Festplattenverschlüsselung. Für diese Endpoints bietet SafeGuard Enterprise verbesserte Challenge/Response Funktionalitäten. Nähere Informationen zu den unterstützten UEFI-Versionen und Beschränkungen hinsichtlich der Unterstützung von SafeGuard BitLocker Challenge/Response finden Sie in den Versionshinweisen unter http://downloads.sophos.com/readmes/readsgn_7_eng.html.

Hinweis: Wenn sich die Beschreibung nur auf UEFI bezieht, ist das explizit angegeben.

Die Tabelle zeigt, welche Komponenten verfügbar sind.

	SafeGuard Festplattenverschlüsselung mit SafeGuard Power-on Authentication (POA)	SafeGuard Power On Authentication (POA) mit C/R Recovery	BitLocker mit Pre-Boot Authentication (PBA), von SafeGuard verwaltet	SafeGuard C/R Wiederherstellung für BitLocker Pre-Boot Authentication (PBA)
Windows 7 BIOS	JA	JA	JA	
Windows 7 UEFI			JA	JA
Windows 8 BIOS			JA	
Windows 8 UEFI			JA	JA

21.1 SafeGuard Festplattenverschlüsselung

Ein Kernstück von SafeGuard Enterprise ist die Verschlüsselung von Daten auf unterschiedlichen Datenträgern. Die Festplattenverschlüsselung kann volume- oder dateibasierend durchgeführt werden, mit unterschiedlichen Schlüsseln und Algorithmen.

Dateien werden transparent verschlüsselt. Wenn Benutzer Dateien öffnen, bearbeiten und speichern, werden sie nicht zur Ver- oder Entschlüsselung aufgefordert.

Als Sicherheitsbeauftragter legen Sie die Einstellungen für die Verschlüsselung in einer Sicherheitsrichtlinie vom Typ **Geräteschutz** fest. Weitere Informationen finden Sie unter Mit Richtlinien arbeiten (Seite 88) und Geräteschutz (Seite 150).

Hinweis: Die in den folgenden Abschnitten beschriebene Funktion der Festplattenvollverschlüsselung kann nur mit Windows 7 BIOS-basierten Systemen genutzt werden. Wenn Sie andere Systeme wie z. B. UEFI oder Windows 8 verwenden, nutzen Sie die integrierte Windows BitLocker Drive Encryption-Funktionalität. Weitere Informationen finden Sie unter BitLocker Drive Encryption (Seite 169).

21.1.1 Volume-basierende Festplattenverschlüsselung

Mit der volume-basierenden Festplattenverschlüsselung werden alle Daten auf einem Volume (einschließlich Boot-Dateien, Pagefiles, Hibernation Files, temporäre Dateien, Verzeichnisinformationen usw.) verschlüsselt. Benutzer müssen sich in ihrer Arbeitsweise nicht anpassen oder auf Sicherheit achten.

Um volume-basierende Verschlüsselung auf Endpoints anzuwenden, erstellen Sie eine Richtlinie vom Typ **Geräteschutz** und wählen Sie bei **Verschlüsselungsmodus für Medien** die Einstellung **Volume-basierend**. Weitere Informationen finden Sie unter Geräteschutz (Seite 150).

Hinweis:

- Die Volume-basierende Verschlüsselung/Entschlüsselung wird für Laufwerke ohne Laufwerksbuchstaben nicht unterstützt.
- Wenn für ein Volume oder einen Volume-Typ eine Verschlüsselungsrichtlinie existiert und die Verschlüsselung des Volumes schlägt fehl, darf der Benutzer nicht auf das Volume zugreifen.
- Endpoints können während der Verschlüsselung/Entschlüsselung heruntergefahren und neu gestartet werden.
- Wenn auf die Entschlüsselung die Deinstallation folgt, empfehlen wir, den Endpoint nicht in einen Energiesparmodus oder den Ruhezustand zu versetzen.
- Wenn nach der volume-basierenden Verschlüsselung eine Richtlinie auf einen Endpoint-Computer angewendet wird, die die Entschlüsselung erlaubt, ist Folgendes zu beachten: Nach einer vollständigen volume-basierenden Verschlüsselung muss der Endpoint-Computer mindestens einmal neu gestartet werden, bevor die Entschlüsselung gestartet werden kann.

Hinweis:

Im Gegensatz zur SafeGuard BitLocker Drive Encryption unterstützt die Volume-basierende SafeGuard-Verschlüsselung keine GUID Partition Table (GPT) Disks. Die Installation wird abgebrochen, wenn eine solche Disk gefunden wird. Wenn dem System später eine GPT Disk hinzugefügt wird, werden Volumes auf der Disk verschlüsselt. Beachten Sie, dass die SafeGuard Recovery-Tools – wie z. B. BE_Restore.exe und recoverkeys.exe – mit solchen Volumes nicht zurechtkommen. Sophos empfiehlt dringend, eine Verschlüsselung von GPT Disks zu vermeiden. Zum Entschlüsseln von Volumes, die unbeabsichtigt verschlüsselt wurden, ändern Sie Ihre SGN-Richtlinien entsprechend und ermöglichen Sie dem Benutzer die Entschlüsselung.

21.1.1.1 Schnelle Initialverschlüsselung

SafeGuard Enterprise bietet die schnelle Initialverschlüsselung als Spezialmodus für die volume-basierende Verschlüsselung. Dieser Modus reduziert den Zeitraum, der für die initiale Verschlüsselung (oder die endgültige Entschlüsselung) von Volumes auf Endpoints benötigt wird. Dies wird dadurch erreicht, dass nur auf den Festplattenspeicherplatz zugegriffen wird, der tatsächlich in Gebrauch ist.

Für die schnelle Initialverschlüsselung gelten folgende Voraussetzungen:

- Die schnelle Initialverschlüsselung funktioniert nur auf NTFS-formatierten Volumes.
- Bei NTFS-formatierten Volumes mit einer Cluster-Größe von 64 KB kann die schnelle Initialverschlüsselung nicht angewendet werden.

Hinweis: Dieser Modus kann zu einem unsichereren Zustand führen, wenn eine Platte vor der Verwendung mit SafeGuard Enterprise bereits in Gebrauch war. Nicht verwendete Sektoren können noch Daten enthalten. Daher ist die schnelle Initialverschlüsselung standardmäßig deaktiviert.

Um die schnelle Initialverschlüsselung zu aktivieren, wählen Sie die Einstellung **Schnelle Initialverschlüsselung** in einer Richtlinie vom Typ **Geräteschutz**.

Hinweis: Für die Entschlüsselung eines Volumes wird unabhängig von der gewählten Richtlinieneinstellung immer die schnelle Initialverschlüsselung verwendet. Für die Entschlüsselung gelten ebenfalls die angegebenen Einschränkungen.

21.1.1.2 Volume-basierende Verschlüsselung und die Windows 7 Systempartition

Für Windows 7 Professional, Enterprise und Ultimate wird auf den Endpoints eine Systempartition angelegt, der kein Laufwerksbuchstabe zugeordnet ist. Diese System-Partition kann nicht von SafeGuard Enterprise verschlüsselt werden.

21.1.1.3 Volume-basierende Verschlüsselung und Unidentified File System Objects

Unidentified File System Objects sind Volumes, die von SafeGuard Enterprise nicht eindeutig als verschlüsselt oder unverschlüsselt identifiziert werden können. Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, so wird der Zugriff auf das Volume verweigert. Existiert keine Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.

Hinweis: Existiert für ein Unidentified File System Object eine Verschlüsselungsrichtlinie, bei der die Richtlinieneinstellung **Schlüssel für die Verschlüsselung** auf eine Option eingestellt ist, die die Schlüsselauswahl ermöglicht (z. B. **Beliebiger Schlüssel im Schlüsselring des Benutzers**), so entsteht zwischen der Anzeige des Schlüsselauswahldialogs und der Verweigerung des Zugriffs auf das Volume eine zeitliche Lücke. Während dieser Zeit kann auf das Volume zugegriffen werden. So lange der Schlüsselauswahldialog nicht vom Benutzer bestätigt wird, besteht Zugriff auf das Volume. Um dies zu vermeiden, geben Sie einen vorausgewählten Schlüssel für die Verschlüsselung an. Weitere Informationen zu den relevanten Richtlinieneinstellungen finden Sie unter Geräteschutz (Seite 150). Diese zeitliche Lücke entsteht auch dann für mit dem Endpoint verbundene Unidentified File System Objects, wenn der Benutzer zu dem Zeitpunkt, an dem die Verschlüsselungsrichtlinie wirksam wird, bereits Dateien auf dem Volume geöffnet hat. In diesem Fall, kann nicht gewährleistet werden, dass der Zugriff auf das Volume verweigert wird, da dies zu Datenverlust führen könnte.

21.1.1.4 Verschlüsselung von Volumes mit aktivierter Autorun-Funktionalität

Wenn Sie auf Volumes, für die die Autorun-Funktionalität aktiviert ist, eine Verschlüsselungsrichtlinie anwenden, so können folgende Probleme auftreten:

- Das Volume wird nicht verschlüsselt.
- Wenn es sich um ein Unidentified File System Object handelt, wird der Zugriff nicht verweigert.

21.1.1.5 Zugriff auf mit BitLocker To Go verschlüsselte Volumes

Wird SafeGuard Enterprise mit aktivierter BitLocker To Go Unterstützung verwendet und existiert eine SafeGuard Enterprise Verschlüsselungsrichtlinie für ein mit BitLocker To Go verschlüsseltes Volume, so wird der Zugriff auf das Volume verweigert. Existiert keine SafeGuard Enterprise Verschlüsselungsrichtlinie, so kann der Benutzer auf das Volume zugreifen.

Weitere Informationen zu BitLocker To Go finden Sie unter BitLocker To Go (Seite 177).

21.1.2 Dateibasierende Festplattenverschlüsselung

Die dateibasierende Verschlüsselung stellt sicher, dass alle Daten verschlüsselt sind (außer Boot Medium und Verzeichnisinformationen). Mit dateibasierender Verschlüsselung lassen sich auch optische Medien wie CD/DVD verschlüsseln. Außerdem können Daten mit Fremdrechnern, auf denen SafeGuard Enterprise nicht installiert ist, ausgetauscht werden (soweit die Richtlinien dies zulassen) (siehe SafeGuard Data Exchange (Seite 193)).

Hinweis: Mit “Dateibasierender Verschlüsselung” verschlüsselte Daten können nicht komprimiert werden. Umgekehrt können auch komprimierte Dateien nicht dateibasierend verschlüsselt werden.

Hinweis: Boot-Volumes werden niemals dateibasierend verschlüsselt. Sie sind automatisch von einer dateibasierenden Verschlüsselung ausgenommen, auch wenn eine entsprechende Regel definiert ist.

Um dateibasierende Verschlüsselung auf Endpoints anzuwenden, erstellen Sie eine Richtlinie vom Typ **Geräteschutz** und wählen Sie bei **Verschlüsselungsmodus für Medien** die Einstellung **Dateibasierend**.

21.1.2.1 Standardverhalten beim Speichern von Dateien

Da sich Anwendungen beim Speichern von Dateien unterschiedlich verhalten, bietet SafeGuard Enterprise zwei Verfahren für das Behandeln von verschlüsselten Dateien, die geändert wurden.

Wurde eine Datei mit einem anderen Schlüssel als dem Standardschlüssel des Volumes verschlüsselt und Sie bearbeiten und speichern die Datei, so würde man erwarten, dass der Verschlüsselungsschlüssel beibehalten wird. Es wurde ja eine Datei bearbeitet, keine neue erstellt. Viele Anwendungen speichern jedoch Dateien, indem sie eine Kombination aus Speichern-, Löschen- und Umbenennen-Vorgängen ausführen (z. B. Microsoft Office). Ist dies der Fall, so verwendet SafeGuard Enterprise in der Standardeinstellung den Standardschlüssel für diesen Verschlüsselungsvorgang und ändert somit den für die Verschlüsselung verwendeten Schlüssel.

Wenn Sie dieses Verhalten ändern und den für die Verschlüsselung verwendeten Schlüssel in jedem Fall beibehalten möchten, können Sie einen Registry Key auf dem Endpoint ändern.

Um den zuvor verwendeten Schlüssel beim Speichern von geänderten Dateien beizubehalten:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]
"ActivateEncryptionTunneling"=dword:00000001
```

Um die Verwendung eines anderen Schlüssels (Standardschlüssel) beim Speichern von geänderten Dateien zuzulassen. Standardeinstellung nach der Installation:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]
"ActivateEncryptionTunneling"=dword:00000000
```

Hinweis: Änderungen an dieser Einstellung werden erst nach einem Neustart des Endpoint wirksam.

21.2 BitLocker Drive Encryption

BitLocker Drive Encryption ist ein in Microsoft Windows Betriebssysteme integriertes Feature für die Festplattenverschlüsselung mit Pre-Boot Authentication. BitLocker bietet Datenschutz durch die Verschlüsselung von Boot- sowie Daten-Laufwerken. Bei Windows 8 und höher kann nur die BitLocker Drive Encryption (nicht die SafeGuard Festplattenverschlüsselung) für die Festplattenverschlüsselung verwendet werden.

SafeGuard Enterprise kann BitLocker Verschlüsselung auf einem Computer verwalten. Die BitLocker-Verschlüsselung kann aktiviert und die Verwaltung von bereits mit BitLocker verschlüsselten Laufwerken übernommen werden.

SafeGuard Enterprise überprüft während der Installation am Endpoint und während dem ersten Neustart, ob die Hardware die Anforderungen für BitLocker mit SafeGuard Challenge/Response erfüllt. Falls nicht, wird die SafeGuard Enterprise BitLocker Verwaltung ohne Challenge/Response ausgeführt. In diesem Fall kann der BitLocker Recovery-Schlüssel mit dem SafeGuard Management Center abgerufen werden.

21.2.1 Authentisierung mit BitLocker-Laufwerkverschlüsselung

Die BitLocker-Laufwerkverschlüsselung bietet verschiedene Authentisierungsoptionen für Boot- und Datenlaufwerke.

Der Sicherheitsbeauftragte kann die verschiedenen Anmeldemodi in einer Richtlinie im SafeGuard Management Center einstellen und sie an die BitLocker Endpoints verteilen.

Für SafeGuard Enterprise BitLocker-Benutzer sind folgende Anmeldemodi verfügbar:

- TPM (nur Boot-Laufwerke)
- TPM + PIN (nur Boot-Laufwerke)
- TPM + Systemstartschlüssel (nur Boot-Laufwerke)
- Kennwort (ohne TPM)
- Systemstartschlüssel (ohne TPM)
- Auto-Unlock (nur Datenlaufwerke)

Weitere Informationen zum Einrichten der Anmeldemodi finden Sie unter Authentisierung (Seite 132).

21.2.1.1 Trusted Platform Module (TPM)

Das TPM ist ein Modul auf dem Motherboard, das einer Smartcard ähnelt und Verschlüsselungsfunktionen sowie Vorgänge für die digitale Signatur ausführt. Es ist in der Lage, Benutzerschlüssel anzulegen, zu speichern und zu verwalten. Das TPM ist gegen Angriffe geschützt.

21.2.1.2 PIN und Kennwörter

Die Voraussetzungen für BitLocker PINs und Kennwörter werden in den Windows Gruppenrichtlinien festgelegt und nicht durch die SafeGuard Enterprise-Einstellungen.

Die betreffenden Einstellungen für Kennwörter sind im lokalen Gruppenrichtlinien-Editor (**gpedit.msc**) zu finden:

Local Computer Policy - Computer Configuration - Administrative Templates - Windows Components - BitLocker Drive Encryption - Operating System Drives - Configure use of passwords for operating system drives und

Local Computer Policy - Computer Configuration - Administrative Templates - Windows Components - BitLocker Drive Encryption - Fixed Data Drives - Configure use of passwords for fixed data drives.

Die Einstellungen können auch über Active Directory angewendet werden.

PINs bestehen in der Regel nur aus Zahlen. Es kann jedoch die Verwendung aller Tastaturzeichen (Zahlen, Buchstaben und Sonderzeichen/Symbole) zugelassen werden. Die Einstellung, mit der diese erweiterten PINs zugelassen werden, ist im lokalen Gruppenrichtlinien-Editor (**gpedit.msc**) unter **Local Computer Policy - Computer Configuration - Administrative Templates - Windows Components - BitLocker Drive Encryption - Operating System Drives** zu finden:

Wenn "Erweiterte PINs für Systemstart zulassen" auf "Aktiviert" gesetzt ist, sind erweiterte PINs zulässig.

Wenn "Erweiterte PINs für Systemstart zulassen" auf "Nicht konfiguriert" gesetzt ist, sind in SafeGuard Enterprise erweiterte PINs zulässig.

Wenn "Erweiterte PINs für Systemstart zulassen" auf "Deaktiviert" gesetzt ist, sind erweiterte PINs nicht zulässig.

Hinweis: BitLocker unterstützt nur das EN-US Tastaturlayout. Benutzer könnten daher Probleme bei der Eingabe erweiterter PINs oder komplexer Kennwörter haben. Wird das Tastaturlayout vor dem Festlegen der neuen BitLocker-PIN oder des neuen Bit Locker-Kennworts nicht in EN-US geändert, muss für die Eingabe des gewünschten Zeichens unter Umständen eine andere Taste gedrückt werden als die auf der Tastatur angegebene. Deshalb wird vor dem Verschlüsseln des Boot-Laufwerks ein Neustart ausgeführt, um sicherzustellen, dass der Benutzer die PIN oder das Kennwort beim Starten korrekt eingeben kann.

21.2.1.3 USB-Stick

Die externen Schlüssel können auf einem ungeschützten USB-Stick gespeichert werden.

21.2.2 Praxistipps: Richtlinieneinstellungen und Bedienung

Der Sicherheitsbeauftragte konfiguriert die Verschlüsselungsrichtlinien für die zu verschlüsselnden Laufwerke sowie eine Authentisierungsrichtlinie. Nach Möglichkeit sollte immer das TPM genutzt werden, aber auch ohne TPM sollte das Boot-Volume verschlüsselt werden. Die Benutzerinteraktion sollte auf ein Minimum beschränkt werden.

Gemäß diesen Anforderungen wählt der Sicherheitsbeauftragte die folgenden Authentisierungseinstellungen (diese sind auch die Standardeinstellungen):

- **BitLocker Anmeldemodus für Boot-Laufwerke**: **TPM + PIN**
- **BitLocker Fallback-Anmeldemodus für Boot-Laufwerke**: **Kennwort oder Systemstartschlüssel:**
- **BitLocker Anmeldemodus für Datenlaufwerke**: **Auto-Unlock**
- **BitLocker Fallback-Anmeldemodus für Datenlaufwerke**: **Kennwort oder Systemstartschlüssel:**

Der Sicherheitsbeauftragte erstellt eine Geräteschutzrichtlinie mit dem Ziel **Interner Speicher** und richtet für den Verschlüsselungsmodus **Volume-basierend** ein. Danach werden beide Richtlinien auf die zu verschlüsselnden Endpoints angewendet.

Für SafeGuard Enterprise BitLocker-Benutzer gibt es folgende Szenarien:

Fall 1: Ein Benutzer meldet sich mit einem TPM bei einem Endpoint an.

1. Der Benutzer wird aufgefordert, eine PIN für das Boot-Volume einzugeben (z. B. Laufwerk C:).
2. Der Benutzer gibt die PIN ein und klickt auf **Neu starten und verschlüsseln**.
3. Das System testet die Hardware und überprüft, ob der Benutzer die PIN korrekt eingeben kann. Es startet neu und fordert den Benutzer zur Eingabe der PIN auf.
   - Wenn der Benutzer die PIN richtig eingibt, wird der Endpoint gestartet.
   - Gibt der Benutzer die PIN nicht richtig ein (z. B. aufgrund eines falschen Tastaturlayouts), kann er die **Esc**-Taste in der BitLocker Pre-Boot-Umgebung drücken, um den Test abzubrechen, und der Endpoint wird gestartet.
   - Falls es ein Problem mit der Hardware gibt (z. B. wenn das TPM nicht funktioniert), wird der Test abgebrochen und der Endpoint gestartet.
4. Der Benutzer meldet sich erneut an.
5. Wenn der Hardware-Test erfolgreich war (der Benutzer konnte die PIN richtig eingeben und es gab kein Problem mit dem TPM), beginnt die Verschlüsselung des Boot-Volume. Andernfalls (wenn der Test fehlschlägt), wird ein Fehler angezeigt und das Volume nicht verschlüsselt. Schlägt der Test fehl, weil der Benutzer **Esc** in der Pre-Boot-Umgebung gedrückt hat, wird der Benutzer aufgefordert, erneut eine PIN einzugeben und einen Neustart vorzunehmen (wie in Schritt 2; die Schritte 3, 4 und 5 werden wiederholt).
6. Die Verschlüsselung des Boot-Volume beginnt.
7. Die Verschlüsselung der Daten-Volumes beginnt ebenfalls, ohne dass eine Interaktion seitens des Benutzers erforderlich ist.

Fall 2: Ein Benutzer meldet sich bei einem Windows 8-Endpoint ohne TPM an.

1. Der Benutzer wird aufgefordert, ein Kennwort für das Boot-Volume einzugeben.
2. Der Benutzer gibt das Kennwort ein und klickt auf **Neu starten und verschlüsseln**.
3. Das System startet neu, führt einen Hardwaretest durch und der Benutzer meldet sich wie im Fall oben erneut an (genau wie in Fall 1, Schritte 3 bis 6, aber die Verweise auf das TPM sind nicht relevant und anstelle einer PIN ist ein Kennwort erforderlich.)

4. Die Verschlüsselung des Boot-Volume beginnt.
5. Die Verschlüsselung der Daten-Volumes beginnt ebenfalls, ohne dass eine Interaktion seitens des Benutzers erforderlich ist.

Fall 3: Ein Benutzer meldet sich bei einem Windows 7-Endpoint ohne TPM an.

1. Der Benutzer wird aufgefordert, den Verschlüsselungsschlüssel für das Boot-Volume auf einem USB-Stick zu speichern.
2. Der Benutzer steckt einen USB-Stick ein und wählt **Speichern und neu starten** aus.
3. Das System startet neu, führt den Hardwaretest durch und der Benutzer meldet sich erneut an. (Gleicher Ablauf wie in den vorgenannten Fällen, aber der Benutzer muss beim Booten den USB-Stick einstecken. Es könnte ein Hardwarefehler auftreten, wenn der USB-Stick von der BitLocker Pre-Boot-Umgebung nicht gelesen werden kann.)
4. Die Verschlüsselung des Boot-Volume beginnt.
5. Die Verschlüsselung der Daten-Volumes beginnt ebenfalls, ohne dass eine Interaktion seitens des Benutzers erforderlich ist.

Fall 4: Der Sicherheitsbeauftragte ändert die Richtlinie und setzt den **BitLocker Fallback-Anmeldemodus für Boot-Laufwerke** auf **Kennwort**. Ein Benutzer meldet sich bei einem Windows 7-Endpoint ohne TPM an.

1. Da der Endpoint kein TPM hat und Windows 7 keine Kennwörter für Boot-Volumes zulässt, wird das Boot-Volume nicht verschlüsselt.
2. Für jedes Nicht-Boot-Volume wird der Benutzer aufgefordert, den externen Schlüssel auf einem USB-Stick zu speichern. Die Verschlüsselung des betreffenden Volume beginnt, sobald der Benutzer auf **Speichern** klickt.
3. Wenn der Benutzer den Endpoint neu startet, muss der USB-Stick eingesteckt sein, damit die Nicht-Boot-Volumes entsperrt werden.

21.2.3 Voraussetzungen für die Verwaltung von BitLocker auf Endpoints

- Um die Anmeldemethoden **TPM + PIN**, **TPM + Systemstartschlüssel**, **Systemstartschlüssel** oder **Kennwort** verwenden zu können, muss die Gruppenrichtlinie **Zusätzliche Authentifizierung beim Start anfordern** entweder in Active Directory oder lokal auf Computern aktiviert werden. Im Editor für lokale Gruppenrichtlinien (gpedit.msc) kann die Gruppenrichtlinie hier gefunden werden:

  Richtlinien für Lokaler Computer\Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\BitLocker Laufwerksverschlüsselung\Betriebssystemlaufwerke

  Um **Systemstartschlüssel** zu verwenden, müssen Sie auch **BitLocker ohne kompatibles TPM zulassen** in den Gruppenrichtlinien aktivieren.

- Um **TPM + PIN** auf Tablets verwenden zu können, müssen Sie auch die Gruppenrichtlinie **Verwendung der BitLocker-Authentifizierung mit erforderlicher Tastatureingabe vor dem Starten auf Slates aktivieren** aktivieren.

  Hinweis: Die Gruppenrichtlinien sind bei der Installation auf dem Endpoint automatisch aktiviert. Stellen Sie sicher, dass die Einstellungen nicht von anderen Gruppenrichtlinien überschrieben werden.

- Eine BitLocker-Geräteschutzrichtlinie, die die Konfiguration eines TPM-basierten Authentifizierungsmechanismus (zum Beispiel **TPM**, **TPM+PIN**, **TPM + Systemstartschlüssel**) auslöst, leitet automatisch die TPM-Aktivierung ein. Der Benutzer wird informiert, dass das TPM aktiviert werden muss, und erhält eine Nachricht, wenn das System neugestartet oder heruntergefahren werden muss (abhängig von dem verwendeten TPM).

Hinweis: Wenn SafeGuard BitLocker Management auf einem Endpoint installiert ist, dann kann **Nicht vorbereitet** als Verschlüsselungsstatus eines Laufwerks angezeigt werden. Das bedeutet, dass das Laufwerk momentan nicht mit BitLocker verschlüsselt werden kann, weil notwendige Vorbereitungen noch nicht durchgeführt wurden. Das trifft nur auf verwaltetete Endpoints zu, weil nicht verwaltetete Endpoints keine Bestandsinformationen melden können.

Siehe auch Registerkarte Laufwerke (Seite 266).

Der Systemstatus kann mit dem Befehlszeilentool SGNState überprüft werden (Administratorberechtigungen erforderlich). Nähere Informationen finden Sie im *SafeGuard Enterprise Tools Guide*. **Volume Info:** Gibt an, ob der Endpoint angemessen für die BitLocker-Verschlüsselung vorbereitet ist oder nicht. In manchen Fällen muss das Windows-Tool zur Laufwerkvorbereitung auf BitLocker ausgeführt werden.

SafeGuard Challenge/Response für BitLocker

Um SafeGuard Enterprise BitLocker Challenge/Response verwenden zu können, müssen die folgenden Voraussetzungen erfüllt sein:

- 64-Bit-Windows
- UEFI Version 2.3.1 oder höher
- Microsoft UEFI Zertifikat ist verfügbar oder Secure Boot ist deaktiviert.
- NVRAM Booteinträge sind von Windows aus zugänglich
- Windows im GPT-Modus installiert
- Die Hardware ist in der POACFG.xml Datei nicht aufgelistet.

  Sophos liefert eine Standard POACFG.xml Datei, die im Setup eingebettet ist. Es wird empfohlen, die neueste Datei herunterzuladen und dem Installationsprogramm bereitzustellen

SafeGuard Enterprise überprüft während der Installation am Endpoint und während dem ersten Neustart, ob die Hardware die Anforderungen für BitLocker mit SafeGuard Challenge/Response erfüllt. Falls nicht, wird die SafeGuard Enterprise BitLocker Verwaltung ohne Challenge/Response ausgeführt. In diesem Fall kann der BitLocker Recovery-Schlüssel mit dem SafeGuard Policy Editor abgerufen werden.

21.2.4 BitLocker Drive Encryption mit SafeGuard Enterprise verwalten

Mit SafeGuard Enterprise können Sie BitLocker Drive Encryption vom SafeGuard Management Center aus verwalten, wie einen nativen SafeGuard Enterprise Client. Als Sicherheitsbeauftragter können Sie Verschlüsselungs- und Authentisierungsrichtlinien einrichten und an die BitLocker-Endpoints verteilen.

Während der Installation des SafeGuard Enterprise-Client auf Windows 7 muss die **BitLocker**-Funktion explizit ausgewählt werden, um die BitLocker-Verwaltung zu ermöglichen.

Sobald ein BitLocker Endpoint bei SafeGuard Enterprise registriert ist, werden Informationen zu Benutzer, Computer, Anmeldemodus und Verschlüsselungsstatus angezeigt. Darüber hinaus werden Ereignisse für BitLocker Clients protokolliert.

Die Verwaltung von BitLocker Clients in SafeGuard Enterprise ist transparent. Das heißt, die Verwaltungsfunktionen haben im Allgemeinen dieselbe Funktionsweise für BitLocker und

native SafeGuard Enterprise Clients. Der Computertyp lässt sich über die Registerkarte **Bestand** eines Containers unter **Benutzer und Computer** ermitteln. Die Spalte **Verschlüsselungstyp** zeigt an, ob es sich bei dem betreffenden Computer um einen BitLocker-Client handelt.

Die zentrale und vollständig transparente Verwaltung von BitLocker durch SafeGuard Enterprise ermöglicht somit die Anwendung in heterogenen IT-Umgebungen. SafeGuard Enterprise erweitert die Funktionalität von BitLocker signifikant. Über SafeGuard Enterprise lassen sich die Sicherheitsrichtlinien für BitLocker zentral ausrollen. Bei der Verwaltung von BitLocker über SafeGuard Enterprise stehen darüber hinaus äußerst wichtige Prozesse, wie Schlüsselverwaltung und Schlüssel-Recovery, zur Verfügung.

Informationen zur SafeGuard Enterprise-Unterstützung der BitLocker To Go-Erweiterung in Windows 7 und 8 finden Sie unter BitLocker To Go (Seite 177).

21.2.5 Verschlüsselung mit dem von SafeGuard Enterprise verwalteten BitLocker

Mit der BitLocker Drive Encryption-Unterstützung in SafeGuard Enterprise können Sie Boot-Volumes und Daten-Volumes mit BitLocker-Verschlüsselung und -Schlüsseln verschlüsseln. Darüber hinaus können Daten, z. B. von Wechselmedien, mit SafeGuard Enterprise dateibasierender Verschlüsselung und SafeGuard Enterprise-Schlüsseln verschlüsselt werden. Dies ist keine BitLocker-Funktion, wird aber von SafeGuard Enterprise bereitgestellt.

21.2.5.1 BitLocker-Verschlüsselungsschlüssel

Bei der Verschlüsselung des Boot-Volumes oder anderer Volumes mit BitLocker über SafeGuard Enterprise werden die Verschlüsselungsschlüssel immer durch BitLocker erzeugt. BitLocker erzeugt jeweils einen Schlüssel für jedes Volume. Dieser Schlüssel lässt sich für keinen anderen Zweck verwenden.

Eine Sicherungskopie des Schlüssels wird in der SafeGuard Enterprise Datenbank gespeichert, wenn BitLocker mit SafeGuard Enterprise verwendet wird. Dies ermöglicht die Einrichtung eines Helpdesk- und Recovery-Mechanismus (ähnlich der SafeGuard Enterprise Challenge/Response Funktionalität).

Es ist jedoch nicht möglich, Schlüssel global auszuwählen oder wiederzuverwenden, wie dies bei nativen SafeGuard Enterprise Clients der Fall ist. Die Schlüssel werden außerdem auch nicht im SafeGuard Management Center angezeigt.

Hinweis: BitLocker erlaubt Ihnen auch, Recovery-Schlüssel im Active Directory zu sichern. Falls dies in den Gruppenrichtlinienobjekten (GPOs) aktiviert ist, dann wird dies automatisch durchgeführt, wenn ein Laufwerk mit BitLocker verschlüsselt ist. Wenn ein Laufwerk bereits verschlüsselt ist, kann der Administrator die BitLocker Recovery-Schlüssel händisch mit dem Windows Manage-BDE tool sichern (siehe "manage-bde -protectors -adbackup -?").

21.2.5.2 BitLocker-Algorithmen in SafeGuard Enterprise

BitLocker unterstützt die folgenden Advanced Encryption Standard (AES) Algorithmen:

- AES-128
- AES-256

AES-128 mit Diffuser und AES-256 mit Diffuser werden nicht mehr unterstützt. Laufwerke, die bereits mit einem Algorithmus mit Diffuser verschlüsselt wurden, können mit SafeGuard Enterprise verwaltet werden.

21.2.5.3 Verschlüsselungsrichtlinien für die BitLocker-Laufwerkverschlüsselung

Der Sicherheitsbeauftragte kann eine Richtlinie für die (Erst-)Verschlüsselung im SafeGuard Management Center anlegen und diese an die BitLocker Endpoints verteilen. Die Richtlinie wird daraufhin auf den Endpoints ausgeführt. Die in der Richtlinie angegebenen Laufwerke werden daraufhin mit BitLocker verschlüsselt.

Da die BitLocker Clients im SafeGuard Management Center transparent verwaltet werden, muss der Sicherheitsbeauftragte keine speziellen BitLocker-Einstellungen für die Verschlüsselung vornehmen. SafeGuard Enterprise kennt den Status der Clients und wählt die BitLocker-Verschlüsselung entsprechend. Wird ein BitLocker Client mit SafeGuard Enterprise installiert und wird die Volume-Verschlüsselung aktiviert, so werden die Volumes durch die BitLocker-Laufwerkverschlüsselung verschlüsselt.

Ein BitLocker Endpoint verarbeitet Richtlinien vom Typ **Geräteschutz** und **Authentisierung**.

Die folgenden Einstellungen werden am Endpoint ausgewertet:

- Einstellungen in einer Richtlinie des Typs **Geräteschutz**:
  - **Ziel:Lokale Datenträger | Interner Speicher | Boot-Laufwerke | Andere Laufwerke | Laufwerksbuchstaben A: -Z:**
  - **Verschlüsselungsmodus für MedienVolume-basierend | Keine Verschlüsselung**
  - **Algorithmus für die VerschlüsselungAES128 | AES256**
  - **Schnelle InitialverschlüsselungJa | Nein**

Nähere Informationen finden Sie unter Geräteschutz (Seite 150).

- Einstellungen in einer Richtlinie des Typs **Authentifizierung**:
  - **BitLocker Anmeldemodus für Boot-Laufwerke:TPM | TPM + PIN | TPM + Systemstartschlüssel | Systemstartschlüssel |**
  - **BitLocker Fallback-Anmeldemodus für Boot-Laufwerke:Systemstartschlüssel | Kennwort | Kennwort oder Systemstartschlüssel | Fehler**
  - **BitLocker Anmeldemodus für Datenlaufwerke**: **Auto-Unlock | Kennwort | Systemstartschlüssel**
  - **BitLocker Fallback-Anmeldemodus für Datenlaufwerke**: **Systemstartschlüssel | Kennwort oder Systemstartschlüssel | Kennwort**

Nähere Informationen finden Sie unter Authentisierung (Seite 132).

Alle anderen Einstellungen werden vom BitLocker Endpoint ignoriert.

21.2.5.4 Verschlüsselung auf einem durch BitLocker geschützten Computer

Vor Beginn der Verschlüsselung werden von BitLocker die Verschlüsselungsschlüssel generiert. Abhängig vom System kann das Verhalten leicht abweichen.

Endpoints mit TPM

Wenn der Sicherheitsbeauftragte einen Anmeldemodus für BitLocker einrichtet, der TPM (TPM, TPM+PIN oder TPM + Systemstartschlüssel) beinhaltet, wird die TPM-Aktivierung automatisch eingeleitet.

Das TPM (Trusted Platform Module) ist ein Hardware-Gerät, das BitLocker zum Speichern seiner Verschlüsselungsschlüssel verwendet. Die Schlüssel werden nicht auf der Festplatte des Computers gespeichert. Während des Startvorgangs muss das BIOS (Basic Input/Output System) auf TPM zugreifen können. Wenn der Benutzer den Computer startet, bezieht BitLocker diese Schlüssel automatisch vom TPM.

Endpoints ohne TPM

Wenn ein Endpoint nicht mit TPM ausgestattet ist, kann ein BitLocker-Systemstartschlüssel oder – falls auf dem Endpoint Windows 8 oder höher ausgeführt wird – ein Kennwort als Anmeldemodus verwendet werden.

Ein BitLocker-Systemstartschlüssel kann mit einem USB-Stick zum Speichern der Verschlüsselungsschlüssel generiert werden. Der Benutzer muss den Stick immer beim Starten des Computers einstecken.

Wenn SafeGuard Enterprise BitLocker aktiviert, werden die Benutzer aufgefordert, den BitLocker-Systemstartschlüssel zu speichern. Es öffnet sich ein Dialog, in dem die gültigen Ziellaufwerke zum Speichern des Systemstartschlüssels angezeigt werden.

Hinweis: Bei Bootlaufwerken ist es wesentlich, dass der Systemstartschlüssel verfügbar ist, wenn Sie den Endpoint starten. Der Systemstartschlüssel kann daher nur auf einem Wechselmedium gespeichert werden.

Bei Daten-Volumes kann der BitLocker-Systemstartschlüssel auf einem verschlüsselten Boot-Volume gespeichert werden. Dies erfolgt automatisch, wenn **Auto-Unlock** in der Richtlinie festgelegt ist.

BitLocker Recovery-Schlüssel

Für die BitLocker Recovery sieht SafeGuard Enterprise ein Challenge/Response-Verfahren vor, das es erlaubt, Informationen vertraulich auszutauschen und die BitLocker Recovery-Schlüssel beim Helpdesk abzurufen (siehe Response für mit BitLocker verschlüsselte SafeGuard Enterprise Clients - UEFI-Endpoints (Seite 254) und Recovery-Schlüssel für mit BitLocker verschlüsselte SafeGuard Enterprise Clients - BIOS-Endpoints (Seite 255)).

Damit Recovery-Vorgänge über Challenge/Response durchgeführt werden können oder ein Abruf des Recovery-Schlüssels möglich ist, müssen die notwendigen Daten dem Helpdesk zur Verfügung gestellt werden. Die für den Recovery-Vorgang erforderlichen Daten werden in spezifischen Schlüssel-Recovery-Dateien gespeichert.

Hinweis: Wenn SafeGuard BitLocker Verwaltung ohne Challenge/Response auf einem Standalone-Endpoint verwendet wird, dann wird der Recovery-Schlüssel nach einem Recovery-Vorgang nicht geändert.

Hinweis: Wenn eine mit BitLocker verschlüsselte Festplatte in einem Computer durch eine neue Festplatte ersetzt wird, diese den Laufwerksbuchstaben der alten Festplatte erhält und ebenfalls mit BitLocker verschlüsselt wird, speichert SafeGuard Enterprise nur den BitLocker Recovery-Schlüssel der neuen Festplatte.

Verwaltung von Laufwerken, die bereits mit BitLocker verschlüsselt sind

Sollte es bei der Installation von SafeGuard Enterprise auf Ihrem Computer Laufwerke geben, die bereits mit BitLocker verschlüsselt sind, übernimmt SafeGuard Enterprise die Verwaltung dieser Laufwerke.

Verschlüsselte Bootlaufwerke

- Abhängig von der verwendeten SafeGuard Enterprise BitLocker Unterstützung werden Sie möglicherweise aufgefordert, Ihren Computer neu zu starten. Es ist wichtig, dass Sie den Neustart so bald als möglich durchführen.
- Wenn für das verschlüsselte Laufwerk eine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:
  - **SafeGuard Enterprise BitLocker Challenge/Response** ist installiert: Die Verwaltung wird übernommen und SafeGuard Enterprise Challenge/Response ist möglich.
  - **SafeGuard Enterprise BitLocker** ist installiert: Die Verwaltung wird übernommen und Recovery ist möglich.
- Wenn für das verschlüsselte Laufwerk keine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:
  - **SafeGuard Enterprise BitLocker Challenge/Response** ist installiert: Es wird keine Verwaltung übernommen und SafeGuard Enterprise Challenge/Response ist nicht möglich.
  - **SafeGuard Enterprise BitLocker** ist installiert: Recovery ist möglich.

Verschlüsselte Festplatten

- Wenn für das verschlüsselte Laufwerk eine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:

  Die Verwaltung wird übernommen und Recovery ist möglich.

- Wenn für das verschlüsselte Laufwerk keine SafeGuard Enterprise-Verschlüsselungsrichtlinie gilt:

  SafeGuard Enterprise Recovery ist möglich.

21.2.5.5 Entschlüsselung mit BitLocker

Computer, die mit BitLocker verschlüsselt wurden, lassen sich nicht automatisch entschlüsseln. Die Entschlüsselung kann entweder über den Menüpunkt **BitLocker Drive Encryption** in der **Systemsteuerung** oder mit dem Microsoft Befehlszeilentool "Manage-bde" ausgeführt werden.

Um Benutzern zu erlauben, mit BitLocker verschlüsselte Laufwerke händisch zu entschlüsseln, muss dem Endpoint eine Richtlinie ohne Verschlüsselungsregel für ein BitLocker verschlüsseltes Laufwerk zugewiesen werden. Der Benutzer kann dann die Entschlüsselung durch Deaktivieren von BitLocker für das gewünschte Laufwerk unter **BitLocker Drive Encryption** in der **Systemsteuerung** auslösen.

21.2.6 BitLocker To Go

Ab Windows 7 wurde die BitLocker -Laufwerkverschlüsselung mit BitLocker To Go erweitert, so dass Benutzer auch Volumes auf Wechselmedien verschlüsseln können. BitLocker To Go kann nicht durch SafeGuard Enterprise verwaltet werden.

BitLocker To Go kann verwendet werden, wenn die Client-Komponenten für SafeGuard Enterprise BitLocker Unterstützung installiert wurden.

Wenn die Client-Komponenten für die volume-basierende Verschlüsselung von SafeGuard Enterprise installiert wurden, dann ist BitLocker To Go nicht kompatibel und wird deaktiviert.

Volumes und Wechselmedien, die vor der Installation von SafeGuard Enterprise mit BitLocker To Go verschlüsselt wurden, bleiben lesbar. Die dateibasierende Verschlüsselung von SafeGuard kann verwendet werden.

21.2.6.1 Deaktivieren der BitLocker To Go Verschlüsselung

1. Wählen Sie im Windows Gruppenrichtlinien-Editor **Local Computer Policy\Computer Configuration\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives**.
2. Unter **Wechseldatenträger** wählen Sie die folgende Richtlinie: **Verwendung von BitLocker auf Wechseldatenträgern steuern**. Setzen Sie die Optionen wie folgt:
   a) Wählen Sie **Aktiviert**.
   b) Deaktivieren Sie unter **Optionen** die Option **Benutzer können BitLocker-Schutz auf Wechseldatenträgern anwenden**.
   c) Wählen Sie unter **Optionen** die Option **Benutzer können BitLocker-Schutz auf Wechseldatenträgern anhalten und entschlüsseln**.
3. Klicken Sie auf **OK**.

BitLocker To Go Verschlüsselung wird auf den Endpoints deaktiviert. Der Benutzer kann neue Laufwerke nicht mehr mit BitLocker To Go verschlüsseln. Laufwerke, die bereits vor Bereitstellung der nativen SafeGuard Enterprise Device Encryption Client-Komponenten mit BitLocker To Go verschlüsselt wurden, bleiben lesbar.

Die Registry-Einstellungen auf dem Client werden folgendermaßen gesetzt:

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\FVE]

"RDVConfigureBDE"=dword:00000001

"RDVAllowBDE"=dword:00000000

"RDVDisableBDE"=dword:00000001

Diese Registry-Einstellungen werden auch während der Installation der SafeGuard Enterprise Device Encryption Client-Komponenten gesetzt. BitLocker To Go wird somit auch auf Computern ohne Domain-Verwaltung (Endpoints in einer Arbeitsgruppe) oder Standalone-Endpoints deaktiviert.

21.2.7 Protokollierung

Vom BitLocker Client gemeldete Ereignisse werden wie für alle anderen SafeGuard Enterprise Clients protokolliert. Dabei wird nicht explizit erwähnt, dass sich das Ereignis auf einen BitLocker Client bezieht. Die Berichte entsprechen den für jeden anderen SafeGuard Enterprise Client erzeugten Berichten.

21.3 FileVault 2 Festplattenverschlüsselung

FileVault 2 ist eine in OS X eingebaute Verschlüsselungstechnogie, die das ganze Laufwerk schützt und von SafeGuard Enterprise verwaltet werden kann.

21.3.1 FileVault 2 Festplattenverschlüsselung mit SafeGuard Enterprise verwalten

Mit SafeGuard Enterprise können Sie FileVault 2 Festplattenverschlüsselung vom SafeGuard Management Center aus verwalten, wie einen nativen SafeGuard Enterprise Client.

Die SafeGuard Enterprise Client Installation beinhaltet nicht auch die Komponente für die Verwaltung von FileVault 2. Sie muss separat installiert werden. Nähere Informationen finden Sie in Ihrer Dokumentation für Sophos SafeGuard Native Device Encryption für Mac.

Die zentrale und vollständig transparente Verwaltung von FileVault2 durch SafeGuard Enterprise ermöglicht die Anwendung in heterogenen IT-Umgebungen. Sicherheitsrichtlinien für verschiedene Plattformen können zentral ausgerollt werden.

21.3.2 Verwalten von FileVault 2 Endpoints im SafeGuard Management Center

Im SafeGuard Management Center lassen sich FileVault 2 Endpoints wie andere native SafeGuard Endpoints verwalten. Als Sicherheitsbeauftragter können Sie Verschlüsselungsrichtlinien für die FileVault 2 Endpoints einrichten und verteilen.

Sobald ein FileVault 2 Endpoint bei SafeGuard Enterprise registriert ist, werden Informationen zu Benutzer, Computer, Anmeldemodus und Verschlüsselungsstatus angezeigt. Darüber hinaus werden Ereignisse für FileVault 2 Clients protokolliert.

Die Verwaltung von FileVault 2 Clients in SafeGuard Enterprise ist transparent. Das heißt, die Verwaltungsfunktionen haben im Allgemeinen dieselbe Funktionsweise für FileVault 2 und native SafeGuard Enterprise Clients. Der Computertyp lässt sich in der Registerkarte **Bestand** eines Containers unter **Benutzer & Computer** ermitteln. Die Spalte **POA-Typ** zeigt an, ob es sich bei dem betreffenden Computer um einen FileVault 2 Client handelt.

21.3.3 Verschlüsselungsrichtlinien für FileVault 2 Festplattenverschlüsselung

Der Sicherheitsbeauftragte kann eine Richtlinie für die Verschlüsselung im SafeGuard Management Center anlegen und diese an die FileVault 2 Endpoints verteilen. Die Richtlinie wird daraufhin auf den Endpoints ausgeführt.

Da die FileVault 2 Endpoints im SafeGuard Management Center transparent verwaltet werden, muss der Sicherheitsbeauftragte keine speziellen FileVault 2-Einstellungen für die Verschlüsselung vornehmen. SafeGuard Enterprise kennt den Status der Clients und wählt die FileVault 2-Verschlüsselung entsprechend.

Ein FileVault 2 Endpoint verarbeitet nur Richtlinien des Typs **Geräteschutz** mit dem Ziel **Boot-Laufwerke** und einem **Verschlüsselungsmodus für Medien**, der auf **Volume-basierend** oder **Keine Verschlüsselung** gesetzt ist. Alle anderen Richtlinieneinstellungen werden ignoriert.

- **Volume-basierend** aktiviert FileVault 2 auf dem Endpoint.
- **Keine Verschlüsselung** erlaubt dem Benutzer den Mac zu entschlüsseln.

22 SafeGuard Configuration Protection

Das Modul SafeGuard Configuration Protection ist ab SafeGuard Enterprise 6.1 nicht mehr verfügbar. Die entsprechende Richtlinie sowie der Suspension Wizard sind im SafeGuard Management Center 7.0 weiterhin für SafeGuard Enterprise 6 oder auch 5.60 Clients mit installiertem Configuration Protection, die mit einem 7.0 Management Center verwaltet werden, verfügbar.

Weitere Informationen zu SafeGuard Configuration Protection finden Sie in der *SafeGuard Enterprise 6 Administratorhilfe*:
http://www.sophos.com/de-de/medialibrary/PDFs/documentation/sgn_60_h_eng_admin_help.pdf.

23 Dateiverschlüsselung

Das SafeGuard Enterprise Modul File Encryption bietet dateibasierende Verschlüsselung auf lokalen Festplatten und im Netzwerk, speziell für Arbeitsgruppen bei Netzwerkfreigaben.

Im SafeGuard Management Center definieren Sie die Regeln für die dateibasierende Verschlüsselung in **File Encryption** Richtlinien. In diesen Richtlinien geben Sie die Zielordner für File Encryption, den Verschlüsselungsmodus und den Schlüssel für die Verschlüsselung an. In Richtlinien vom Typ **Allgemeine Einstellungen** können Sie festlegen, wie bestimmte Anwendungen und Dateisysteme auf Endpoints in Zusammenhang mit File Encryption behandelt werden sollen. Sie können ignorierte und vertrauenswürdige Anwendungen sowie ignorierte Geräte angeben. Außerdem können Sie die persistente Verschlüsselung für File Encryption aktivieren.

Für die Verschlüsselung können persönliche Schlüssel verwendet werden. Ein persönlicher Schlüssel, der für einen Benutzer aktiv ist, gilt nur für diesen bestimmten Benutzer und kann nicht anderen Benutzern zugewiesen oder mit diesen gemeinsam benutzt werden. Sie können persönliche Schlüssel im SafeGuard Management Center unter **Benutzer & Computer** erzeugen.

Wenn Endpoints eine **File Encryption** Richtlinie zugewiesen wurde, werden die Dateien in den von der Richtlinie abgedeckten Speicherorten ohne Benutzerinteraktion transparent verschlüsselt:

- Neue Dateien in den relevanten Speicherorten werden automatisch verschlüsselt.
- Wenn Benutzer den Schlüssel für eine verschlüsselte Datei haben, können sie den Inhalt lesen und ändern.
- Wenn Benutzer den Schlüssel für eine verschlüsselte Datei nicht haben, wird der Zugriff verweigert.
- Wenn ein Benutzer auf einem Endpoint, auf dem File Encryption nicht installiert ist, auf eine verschlüsselte Datei zugreift, wird der verschlüsselte Inhalt angezeigt.

Sind in den durch die Verschlüsselungsrichtlinie abgedeckten Speicherorten bereits Dateien vorhanden, so werden diese nicht automatisch verschlüsselt. Die Benutzer müssen auf dem Endpoint eine Initialverschlüsselung im **SafeGuard Assistent für Dateiverschlüsselung** durchführen. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Benutzerhilfe*.

Hinweis:

SafeGuard File Encryption ist mit der in Windows integrierten EFS-Verschlüsselung und Dateikomprimierung nicht kompatibel. Wenn die EFS-Verschlüsselung aktiviert ist, erhält sie Priorität vor etwaig anwendbaren File Encryption Verschlüsselungsregeln. In den relevanten Ordnern angelegte Dateien können in diesem Fall nicht von File Encryption verschlüsselt werden. Wenn die Komprimierung aktiviert ist, hat die Verschlüsselung durch File Encryption eine höhere Priorität. Dateien werden verschlüsselt, jedoch nicht komprimiert. Um Dateien mit File Encryption zu verschlüsseln, muss die EFS-Verschlüsselung oder die Komprimierung zunächst deaktiviert werden. Dies kann manuell oder durch Ausführen des SafeGuard Enterprise Assistenten für die Initialverschlüsselung erfolgen.

Hinweis:

Nähere Informationen bei Verwendung von Mac Endpoints und SafeGuard File Encryption for Mac entnehmen Sie den folgenden Dokumenten:

- *SafeGuard File Encryption for Mac - Schnellstartanleitung.*

Dieses Dokument ist an Mac Benutzer gerichtet.

- *SafeGuard File Encryption for Mac - Administratorhilfe.*

  Dieses Dokument ist für Administratoren vorgesehen, die mit beiden Plattformen, Mac und Windows, arbeiten.

23.1 Konfigurieren von Verschlüsselungsregeln in File Encryption Richtlinien

Die Regeln für die dateibasierende Verschlüsselung im Netzwerk definieren Sie in einer Richtlinie des Typs **File Encryption**.

Hinweis: Wenn bestimmte Ordner verschlüsselt werden (zum Beispiel C:\Programme), bewirkt dies unter Umständen, dass das Betriebssystem oder bestimmte Anwendungen nicht mehr laufen. Stellen Sie bei der Definition von Verschlüsselungsregeln sicher, dass diese Ordner nicht verschlüsselt werden.

1. Legen Sie im **Richtlinien** Navigationsbereich einen neue Richtlinie vom Typ **File Encryption** an oder wählen Sie eine vorhandene aus.

   Die Tabelle für **File Encryption** Richtlinienregeln wird angezeigt.

2. Geben Sie in der Spalte **Pfad** den Pfad (d. h. den Ordner) an, der durch File Encryption verschlüsselt werden soll:

   - Klicken Sie auf die Dropdown-Schaltfläche und wählen Sie einen Platzhalter für einen Ordnernamen aus der Liste der verfügbaren Platzhalter aus.

     Hinweis: Wenn Sie Ihren Cursor über die Listeneinträge führen, werden Tooltips angezeigt, die zeigen, wie ein Platzhalter üblicherweise auf einem Endpoint umgesetzt wird. Geben Sie nur gültige Platzhalter ein. Eine Beschreibung aller verfügbaren Platzhalter finden Sie unter Platzhalter für Pfade in File Encryption Verschlüsselungsregeln (Seite 185).

     Hinweis: Die Verschlüsselung des gesamten Benutzerprofils mit dem Platzhalter <User Profile> kann zu einem instabilen Windows Desktop auf dem Endpoint führen.

   - Klicken Sie auf die Browse-Schaltfläche um den gewünschten Ordner im Dateisystem auszuwählen.
   - Sie können auch einfach einen Pfadnamen eingeben.

   Hinweis: Nützliche Informationen zum Konfigurieren von Pfaden in Dateiverschlüsselungsregeln finden Sie unter Zusätzliche Informationen für die Konfiguration von Pfaden in File Encryption Verschlüsselungsregeln (Seite 183).

3. Wählen Sie in der Spalte **Anwendungsbereich**:

   - **Nur dieser Ordner**, um die Regeln nur auf den Ordner anzuwenden, der in der Spalte **Pfad** angegeben ist, oder
   - **Mit Unterordnern**, um die Regel auch auf alle Unterordner des Ordners anzuwenden.

4. Legen Sie in der Spalte **Modus** fest, wie File Encryption den in der Spalte **Pfad** angegebenen Ordner behandeln soll:

   - Wählen Sie **Verschlüsseln**, um neue Dateien im Ordner zu verschlüsseln. Der Inhalt der vorhandenen verschlüsselten Dateien wird transparent entschlüsselt, wenn ein Benutzer mit dem erforderlichen Schlüssel auf die Dateien zugreift. Hat der Benutzer nicht den erforderlichen Schlüssel, wird der Zugriff verweigert.

   - Wenn Sie **Ausschließen** auswählen, werden neue Dateien im Ordner nicht verschlüsselt. Sie können diese Option verwenden, wenn Sie zum Beispiel einen Unterordner von der Verschlüsselung ausnehmen möchten, dessen übergeordneter Ordner bereits von einer Regel mit der Option **Verschlüsseln** abgedeckt ist.
   - Wenn Sie **Ignorieren** auswählen, werden die Dateien im Ordner von File Encryption nicht beachtet. Neue Dateien werden im Klartext gespeichert. Wenn ein Benutzer auf bereits verschlüsselte Dateien in diesem Ordner zugreift, wird der verschlüsselte Inhalt angezeigt. Dabei spielt es keine Rolle, ob der Benutzer den erforderlichen Schlüssel hat oder nicht.

5. Wählen Sie in der Spalte **Schlüssel** den Schlüssel, der für den **Verschlüsseln** Modus verwendet werden soll. Sie können Schlüssel verwenden, die in **Benutzer & Computer** erstellt und angewendet wurden.

   - Klicken Sie auf die Browse-Schaltfläche, um den Dialog **Schlüssel suchen** zu öffnen. Klicken Sie auf **Jetzt suchen**, um eine Liste mit allen verfügbaren Schlüsseln aufzurufen. Wählen Sie den gewünschten Schlüssel aus.

     Hinweis: Computerschlüssel werden in dieser Liste nicht angezeigt. Sie können von File Encryption nicht benutzt werden, da sie nur auf einem einzelnen Computer verfügbar sind. Mit diesen Schlüssel können daher Benutzergruppen nicht auf dieselben Daten zugreifen.

   - Klicken Sie auf die Schaltfläche **Persönlicher Schlüssel** mit dem Schlüsselsymbol, um den Platzhalter **Persönlicher Schlüssel** in die Spalte **Schlüssel** einzufügen. Auf dem Endpoint wird dieser Platzhalter in den aktiven persönlichen Schlüssel des angemeldeten SafeGuard Enterprise Benutzers umgesetzt. Wenn die relevanten Benutzer noch keine aktiven persönlichen Schlüssel haben, werden diese automatisch angelegt. Sie können persönliche Schlüssel für einzelne oder mehrere Benutzer unter **Benutzer & Computer** erzeugen. Weitere Informationen finden Sie unter Persönliche Schlüssel für die dateibasierende Verschlüsselung mit File Encryption (Seite 74).

6. Der **System** Typ (**Windows**, **Mac OS X** oder **Alle Plattformen** für Windows und Mac OSX systems) werden automatisch zugewiesen.
7. Fügen Sie je nach Anforderung weitere Verschlüsselungsregeln hinzu und speichern Sie Ihre Änderungen.

   Hinweis: Alle File Encryption Verschlüsselungsregeln, die über Richtlinien zugewiesen und für Benutzer/Computer an unterschiedlichen Knoten unter **Benutzer & Computer** aktiviert werden, werden kumuliert. Die Reihenfolge der Verschlüsselungsregeln innerhalb einer **File Encryption** Richtlinie ist für die Evaluierung auf dem Endpoint nicht von Bedeutung. Innerhalb einer **File Encryption** Richtlinie können Sie die Regeln durch Ziehen mit der Maus zur besseren Übersicht nach Wunsch anordnen.

23.1.1 Zusätzliche Informationen für die Konfiguration von Pfaden in File Encryption Verschlüsselungsregeln

Beachten Sie beim Konfigurieren von Pfaden in File Encryption Verschlüsselungsregeln die folgenden Informationen:

- Ein Pfad darf nur Zeichen enthalten, die auch in Dateisystemen verwendet werden können. Zeichen wie <, >, * und $ sind nicht zulässig.
- Geben Sie nur gültige Platzhalter ein. Eine Liste aller unterstützten Platzhalter finden Sie unter Platzhalter für Pfade in File Encryption Verschlüsselungsregeln (Seite 185).

  Hinweis: Die Namen von Umgebungsvariablen werden durch das SafeGuard Management Center nicht überprüft. Sie müssen nur auf dem Endpoint vorhanden sein.

- Das Feld **Pfad** gibt immer einen Ordner an. Sie können keine Regel für eine einzelne Datei festlegen. Außerdem können Sie keine Platzhalter für Ordnernamen, Dateinamen oder Dateierweiterungen verwenden.
- **Absolute und relative Regeln**

  Sie können absolute und relative Regeln definieren. Eine absolute Regel definiert einen bestimmten Ordner, zum Beispiel **`C:\encrypt`**. Eine relative Regel enthält keine UNC Server/Freigabe Informationen, Laufwerksbuchstaben oder Informationen zu übergeordneten Ordnern. In einer relativen Regel wird zum Beispiel ein Pfad wie der folgende verwendet: **`encrypt_sub`**. In diesem Fall werden alle Dateien auf allen Laufwerken (einschließlich Speicherorte im Netzwerk), die sich in einem Ordner mit der Bezeichnung **`encrypt_sub`** (oder in einem untergeordneten Ordner) befinden, von der Regel abgedeckt.

- **Lange Ordnernamen und 8.3 Notation**

  Geben Sie für File Encryption Verschlüsselungsregeln immer die langen Ordnernamen an, da die 8.3 Bezeichnungen für lange Ordnernamen von Computer zu Computer unterschiedlich sein können. 8.3 Namensregeln werden vom durch SafeGuard Enterprise geschützten Endpoint automatisch bei Anwendung der relevanten Richtlinien erkannt. Es sollte keine Rolle spielen, ob Anwendungen lange Ordnernamen oder 8.3 Namen für den Zugriff auf Dateien verwenden. Verwenden Sie für relative Regeln kurze Ordnernamen um sicherzustellen, dass die Regel umgesetzt werden kann, egal ob eine Anwendung lange Ordnernamen oder 8.3 Notation verwendet.

- **UNC und verbundene Laufwerke**

  Ob Sie Regeln in UNC Notation oder basierend auf verbundenen Laufwerksbuchstaben anwenden, hängt von Ihren spezifischen Anforderungen ab:

  - Verwenden Sie UNC Notation, wenn sich die Server- und Freigabenamen wahrscheinlich nicht ändern, die verbundenen Laufwerksbuchstaben jedoch von Benutzer zu Benutzer unterschiedlich sein können.
  - Verwenden Sie verbundene Laufwerksbuchstaben, wenn diese unverändert beibehalten werden, Servernamen aber geändert werden können.

  Wenn Sie UNC verwenden, geben Sie einen Servernamen und einen Freigabenamen an, zum Beispiel \\server\share.

  File Encryption gleicht die UNC Namen und die verbundenen Laufwerksbuchstaben intern ab. In einer Regeln muss ein Pfad somit entweder als UNC-Pfad oder mit verbundenen Laufwerksbuchstaben definiert sein.

  Hinweis: Da Benutzer u. U. ihre verbundenen Laufwerksbuchstaben ändern können, empfehlen wir, aus Sicherheitsgründen UNC-Pfade in File Encryption Verschlüsselungsregeln zu verwenden.

- **Offline-Ordner**

  Bei Anwendung der Windows Funktion **Offline verfügbar machen** müssen Sie keine speziellen Regeln für lokale (Offline) Kopien von Ordnern erstellen. Neue Dateien in der lokalen Kopie eines Ordners, der offline verfügbar gemacht wurde, werden entsprechend den Regeln für den ursprünglichen (Netzwerk-)Speicherplatz verschlüsselt.

Hinweis: Für weitere Informationen zur Bennungn von Dateien und Pfade, siehe http://msdn.microsoft.com/en-us/library/aa365247.aspx.

23.1.2 Platzhalter für Pfade in File Encryption Verschlüsselungsregeln

Beim Angeben von Pfaden in Verschlüsselungsregeln in **File Encryption** Richtlinien können die folgenden Platzhalter verwendet werden. Um diese Platzhalter auszuwählen, klicken Sie auf die Dropdown-Schaltfläche des Felds **Pfad**.

Pfad-Platzhalter	Betriebssystem (Alle=Windows und Mac OS X)	Wert auf dem Endpoint
<%environment_variable_name%>	Alle	Wert der Umgebungsvariable. Beispiel: <%USERNAME%>. **Hinweis:** Wenn Umgebungsvariablen mehrere Speicherorte enthalten (zum Beispiel die PATH Umgebungsvariable), werden die Pfade nicht in mehrere Regeln aufgeteilt. Dies verursacht einen Fehler und die Verschlüsselungsregel ist ungültig.
<Desktop>	Windows	Der virtuelle Ordner für das Microsoft Windows Desktop
<Documents>	Alle	Das ist der virtuelle Ordner für den Desktop-Bereich Eigene Dateien (Äquivalent zu CSIDL_MYDOCUMENTS). Typischer Pfad: C:\Documente und Einstellungen\Benutzername\Eigene Dateien.
<Downloads>	Alle	Der Ordner in dem standardmäßig Downloads gespeichert werden. Ein typischer Pfad unter Windows ist C:\Benutzer\Benutzername\Downloads.
<Music>	Alle	Das Dateisystemverzeichnis, das als allgemeines Repository für Musikdateien dient. Typischer Pfad: C:\Documente und Einstellungen\Benutzername\Eigene Dateien\Eigene Musik.
<Pictures>	Alle	Das Dateisystemverzeichnis, das als allgemeines Repository für Bilddateien dient. Typischer Pfad: C:\Documente und Einstellungen\Benutzername\Eigene Dateien\Eigene Bilder.
<Public>	Alle	Das Dateisystemverzeichnis, das als allgemeines Repository für Dokumente für alle Benutzer dient. Typischer Pfad: C:\Benutzer\<Benutzername>\Öffentlich.
<User Profile>	Alle	Der Profilordner des Benutzers. Typischer Pfad: C:\Benutzer\Benutzername. **Hinweis:** Die Verschlüsselung des gesamten Benutzerprofils mit diesem

Pfad-Platzhalter	Betriebssystem (Alle=Windows und Mac OS X)	Wert auf dem Endpoint
		Platzhalter kann zu einem instabilen Windows Desktop auf dem Endpoint führen.
<Videos>	Alle	Das Dateisystemverzeichnis, das als allgemeines Repository für Videodateien für alle Benutzer dient. Typischer Pfad: C:\Documente und Einstellungen\Alle Benutzer\Dateien\Eigene Videos.
<Cookies>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für Internet Cookies dient. Typischer Pfad: C:\Documente und Einstellungen\Benutzername\Cookies.
<Favorites>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für die Favoriten des Benutzers dient. Typischer Pfad: C:\Documente und Einstellungen\Benutzername\Favoriten.
<Local Application Data>	Windows	Das Dateisystemverzeichnis, das als allgemeines Daten-Repository für lokale Applikationen (ohne Roaming) dient. Typischer Pfad: C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Anwendungsdaten.
<Program Data>	Windows	Das Dateisystemverzeichnis, das Anwendungsdaten für alle Benutzer enthält. Typischer Pfad: C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten.
<Program Files>	Windows	Der Programme-Ordner. Typischer Pfad: \Programme. For 64-Bit Systeme wird dies auf zwei Regeln erweitert: eine für 32-Bit Anwendungen und eine für 64-Bit Anwendungen.
<Public Music>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für Musikdateien für alle Benutzer dient. Typischer Pfad: C:\Documente und Einstellungen\Alle Benutzer\Eigene Musik.
<Public Pictures>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für Bilddateien für alle Benutzer dient. Typischer Pfad: C:\Documente und Einstellungen\Alle Benutzer\Dateien\Eigene Bilder.

Pfad-Platzhalter	Betriebssystem (Alle=Windows und Mac OS X)	Wert auf dem Endpoint
<Public Videos>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für Videodateien für alle Benutzer dient. Typischer Pfad: C:\Documente und Einstellungen\Alle Benutzer\Dateien\Eigene Videos.
<Roaming>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für anwendungsspezifische Daten dient. Typischer Pfad: C:\Dokumente und Einstellungen\Benutzername\Anwendungsdaten.
System	Windows	Der Windows Systemordner. Typischer Pfad: C:\Windows\System32. For 64-Bit Systeme wird dies auf zwei Regeln erweitert: eine für 32-Bit und eine für 64-Bit.
<Temporary Burn Folder>	Windows	Das Dateisystemverzeichnis, das als Staging-Bereich für Dateien, die auf eine CD geschrieben werden sollen, verwendet wird. Typischer Pfad: C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Microsoft\CD Burning.
<Temporary Internet Folder>	Windows	Das Dateisystemverzeichnis, das als allgemeines Repository für temporäre Internetdateien dient. Typischer Pfad: C:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Temporary Internet Files.
<Windows>	Windows	Das Windows-Verzeichnis oder SYSROOT. Dies entspricht den Umgebungsvariablen %windir% oder %SYSTEMROOT%. Typischer Pfad: C:\Windows.
<Removables>	Mac OS X	Zeigt auf die Root-Verzeichnisse aller Mac OS X Wechselmedien.
<Root>	Mac OS X	Mac OS X Stammverzeichnis. Es wird nicht empfohlen, Richtlinien für das Stammverzeichnis festzulegen, auch wenn dies technisch möglich ist.

Hinweis: Verwenden Sie immer Backslashes als Separatoren, auch wenn Sie Dateiverschlüsselungsregeln für Mac OS X festlegen. Auf diese Weise können Sie Regeln auf beiden Betriebssystemen (Windows und Mac OS X) anwenden.

Hinweis: Am Mac OS X Client werden die umgekehrten Schrägstriche automatisch in Schrägstriche umgewandelt, um die Anforderungen des Mac OS X Betriebssystems zu erfüllen. Fehler bei der Verwendung von Platzhaltern werden protokolliert. Ungültige Verschlüsselungsregeln werden protokolliert und dann auf dem Endpoint verworfen.

Beispiel für eine Pfadumwandlung

Der folgende Windows Pfad

<User Profile>\Dropbox\personal

wird auf Mac Seite konvertiert in

/Users/<Username>/Dropbox/personal

23.2 Konfigurieren von Dateiverschlüsselungseinstellungen in Richtlinien vom Typ Allgemeine Einstellungen

Neben den in **File Encryption** Richtlinien definierten Verschlüsselungsregeln können Sie in Richtlinien vom Typ **Allgemeine Einstellungen** folgende Einstellungen für die **Dateiverschlüsselung** konfigurieren:

- **Vertrauenswürdige Anwendungen**
- **Ignorierte Anwendungen**
- **Ignorierte Geräte**
- **Persistente Verschlüsselung aktivieren**

23.2.1 Konfigurieren von vertrauenswürdigen und ignorierten Anwendungen für File Encryption

Sie können Anwendungen als vertrauenswürdig definieren, um ihnen Zugriff auf verschlüsselte Dateien zu geben. Dies ist zum Beispiel notwendig, damit Antivirus-Software verschlüsselte Dateien überprüfen kann.

Sie können Anwendungen als ignoriert definieren, um sie von der transparenten Dateiverschlüsselung/Dateientschlüsselung auszuschließen. Wenn Sie zum Beispiel ein Backup-Programm als ignorierte Anwendung definieren, bleiben die vom Programm gesicherten verschlüsselten Daten verschlüsselt.

Hinweis: Untergeordnete Prozesse werden nicht als vertrauenswürdig/ignoriert eingestuft.

1. Legen Sie im **Richtlinien** Navigationsbereich einen neue Richtlinie vom Typ **Allgemeine Einstellungen** an oder wählen Sie eine vorhandene aus.
2. Klicken Sie unter **Dateiverschlüsselung** auf die Dropdown-Schaltfläche der Felder **Vertrauenswürdige Anwendungen** oder **Ignorierte Anwendungen**.

3. Geben Sie im Editor-Listenfeld die Anwendungen ein, die Sie als vertrauenswürdig/ignoriert definieren möchten.
   - Sie können mehrere vertrauenswürdige/ignorierte Anwendungen in einer Richtlinie definieren. Jede Zeile im Editor-Listenfeld definiert jeweils eine Anwendung.
   - Anwendungsnamen müssen auf .exe enden.
   - Anwendungsnamen müssen als Fully Qualified Paths mit Laufwerk/Verzeichnis definiert werden, zum Beispiel "c:\dir\beispiel.exe". Es reicht nicht aus, nur den Dateinamen einzugeben (zum Beispiel "beispiel.exe"). Aus Gründen der Benutzerfreundlichkeit zeigt die Einzelzeilenansicht der Anwendungsliste nur die Dateinamen getrennt durch Strichpunkte.
   - Die Anwendungsnamen können dieselben Platzhalter für Windows Shell Ordner und Umgebungsvariablen wie die Verschlüsselungsregeln in File Encryption Richtlinen enthalten. Eine Beschreibung aller verfügbaren Platzhalter finden Sie unter Platzhalter für Pfade in File Encryption Verschlüsselungsregeln (Seite 185).
4. Speichern Sie Ihre Änderungen.

Hinweis: Die Richtlinieneinstellungen **Vertrauenswürdige Anwendungen** und **Ignorierte Anwendungen** sind Computereinstellungen. Die Richtlinie muss daher Computern, nicht Benutzern, zugewiesen werden. Andernfalls werden die Einstellungen nicht wirksam.

23.2.2 Konfigurieren von ignorierten Geräten für File Encryption

Sie können Geräte als ignoriert definieren, um sie von der Dateiverschlüsselung auszuschließen. Sie können nur vollständige Geräte ausschließen.

1. Legen Sie im **Richtlinien** Navigationsbereich einen neue Richtlinie vom Typ **Allgemeine Einstellungen** an oder wählen Sie eine vorhandene aus.
2. Klicken Sie unter **Dateiverschlüsselung** auf die Dropdown-Schaltfläche des Felds **Ignorierte Geräte**.
3. Führen Sie im Editor-Listenfeld folgende Schritte durch:

   a) Wählen Sie **Netzwerk** wenn Sie keine Daten am Netzwerk verschlüsseln wollen.

   b) Geben Sie die entsprechenden Gerätenamen an, um spezifische Geräte von der Verschlüsselung auszuschließen. Dies ist zum Beispiel nützlich, wenn Sie Systeme von Dritt-Anbietern ausschließen müssen.

   Hinweis: Sie können die Namen der derzeit im System benutzten Geräte mit Tools von Dritt-Anbietern (z. B. OSR Device Tree) anzeigen lassen. SafeGuard Enterprise protokolliert alle Geräte, mit denen eine Verbindung hergestellt wird. Mit Hilfe von Registry Keys können Sie eine Liste von verbundenen und ignorierten Geräten aufrufen. Weitere Informationen finden Sie unter Anzeige von ignorierten und verbundenen Geräten für die File Encryption-Konfiguration (Seite 190).

   Sie können einzelne (Netzwerk)-Festplattenlaufwerke von der Verschlüsselung ausschließen, in dem Sie eine File Encryption Verschlüsselungsregel in einer **File Encryption** Richtlinie erstellen und den **Modus** für die Verschlüsselung auf **Ignorieren** einstellen. Sie können diese Einstellung nur auf durch Windows verwaltete Laufwerke, nicht auf Mac OS X Volumes.

23.2.2.1 Anzeigen von ignorierten und verbundenen Geräten für die File Encryption Konfiguration

Als Hilfestellung für die Definition von ignorierten Geräten können Sie mit Registry Keys ermitteln, welche Geräte für die Verschlüsselung in Betracht gezogen werden (verbundene Geräte) und welche Geräte derzeit ignoriert werden. Die Liste mit ignorierten Geräten enthält nur Geräte, die tatsächlich auf dem Computer verfügbar sind und ignoriert werden. Wird ein Gerät in einer Richtlinie als ignoriert definiert und das Gerät ist nicht verfügbar, so wird das Gerät auch nicht aufgelistet.

Benutzen Sie folgende Registry Keys, um verbundene und ignorierte Geräte zu ermitteln:

- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\AttachedDevices`**
- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\IgnoredDevices`**

23.2.3 Konfigurieren der persistenten Verschlüsselung für File Encryption

Der Inhalt von mit File Encryption verschlüsselten Dateien wird jeweils direkt entschlüsselt, wenn der Benutzer den erforderlichen Schlüssel hat. Wenn der Inhalt in einer neuen Datei an einem Ablageort gespeichert wird, für den keine Verschlüsselungsregel gilt, bleibt die resultierende neue Datei unverschlüsselt.

Mit persistenter Verschlüsselung bleiben Kopien von verschlüsselten Dateien auch dann verschlüsselt, wenn sie an einem Speicherort abgelegt werden, für den keine Verschlüsselungsregel gilt.

Sie können die persistente Verschlüsselung in Richtlinien vom Typ **Allgemeine Einstellungen** konfigurieren. Die Richtlinieneinstellung **Persistente Verschlüsselung aktivieren** ist standardmäßig aktiviert.

Hinweis: Wenn Dateien an ein ignoriertes Gerät oder in einen Ordner kopiert oder verschoben werden, für den eine Richtlinie mit dem Modus für die Verschlüsselung **Ignorieren** gilt, hat die Einstellung **Persistente Verschlüsselung aktivieren** keine Auswirkungen.

23.3 Mehrere File Encryption Richtlinien

Alle File Encryption Verschlüsselungsregeln, die über Richtlinien zugewiesen und für Benutzer/Computer an unterschiedlichen Knoten unter **Benutzer & Computer** im SafeGuard Management Center aktiviert werden, werden kumuliert.

Sie können eine allgemeine **File Encryption** Richtlinie mit Regeln, die für alle Benutzer relevant sind, am Stammverzeichnisknoten und Richtlinien für spezifischere Anforderungen an den einzelnen Unterknoten zuweisen. Alle Regeln aus allen Richtlinien, die Benutzern/Computern zugewiesen sind, werden kumuliert und treten auf dem Endpoint in Kraft.

23.3.1 File Encryption Richtlinien im RSOP

Wenn für einen Benutzer/Computer mehrere **File Encryption** Richtlinien gelten, zeigt die Registerkarte **RSOP** (Resulting Set of Policies) unter **Benutzer & Computer** die Summe aller File Encryption Verschlüsselungsregeln aus allen **File Encryption** Richtlinien an. Die Regeln werden in der Reihenfolge ihrer Evaluierung auf dem Endpoint-Computer sortiert (siehe Reihenfolge der Evaluierung von File Encryption Verschlüsselungsregeln auf Endpoints (Seite 191)).

Die Spalte **Name der Richtlinie** gibt an, woher die einzelnen Regeln stammen.

Für doppelte Regeln wird die zweite (und dritte usw.) Regel mit einem Symbol markiert. Dieses Symbol bietet auch einen Tooltip, der Sie informiert, das die Regel auf dem Endpoint verworfen wird, da sie ein Duplikat einer Regel mit einer höheren Priorität ist.

23.4 Reihenfolge der Evaluierung von File Encryption Verschlüsselungsregeln auf Endpoints

File Encryption Verschlüsselungsregeln werden auf Endpoints in einer Reihenfolge sortiert, die bewirkt, dass genauer definierte Speicherorte zuerst evaluiert werden.

- Wenn zwei Regeln mit den gleichen Einstellungen für **Pfad** und **Anwendungsbereich** aus Richtlinien stammen, die unterschiedlichen Knoten zugewiesen sind, wird die Regel aus der Richtlinie angewendet, die sich näher am Benutzerobjekt in **Benutzer & Computer** befindet.
- Wenn zwei Regeln mit den gleichen Einstellungen für **Pfad** und **Anwendungsbereich** aus Richtlinien stammen, die demselben Knoten zugewiesen sind, wird die Regel aus der Richtlinie mit der höchsten Priorität angewendet.
- Absolute Regeln werden vor relativen Regeln evaluiert, zum Beispiel **`c\encrypt`** vor **`encrypt`**. Weitere Informationen finden Sie unter Zusätzliche Informationen für die Konfiguration von Pfaden in File Encryption-Verschlüsselungsregeln (Seite 183).
- Regeln mit einem Pfad mit mehr Unterverzeichnissen werden vor Regeln mit einem Pfad mit weniger Unterverzeichnissen evaluiert.
- Mit UNC definierte Regeln werden vor Regeln mit Laufwerksbuchstabeninformationen evaluiert.
- Regeln, bei denen die Option **Nur dieser Ordner** aktiviert ist, werden vor Regeln ohne diese Option evaluiert.
- Regeln mit dem Modus **Ignorieren** werden vor Regeln mit dem Modus **Verschlüsseln** oder **Ausschließen** evaluiert.
- Regeln mit dem Modus **Ausschließen** werden vor Regeln mit dem Modus **Verschlüsseln** evaluiert.
- Wenn bei zwei Regeln die aufgelisteten Kriterien übereinstimmen, werden die Regeln in alphabetischer Reihenfolge evaluiert.

23.5 Konflikte bei File Encryption Regeln

Da einem Benutzer/Computer mehrere File Encryption Richtlinien zugewiesen werden können, treten u. U. Konflikte auf. Ein Regelkonflikt besteht, wenn die Regeln dieselben Werte für Pfad, Modus und Unterverzeichnis enthalten, jedoch unterschiedliche Schlüssel. In diesem Fall gilt die Regel aus der File Encryption Richtlinie mit der höheren Priorität. Die andere Regel wird verworfen.

23.6 File Encryption und SafeGuard Data Exchange

Mit SafeGuard Data Exchange lassen sich Daten, die auf mit Endpoint-Computern verbundenen Wechselmedien gespeichert werden, verschlüsseln und mit anderen Benutzern austauschen. Für SafeGuard Data Exchange wird dateibasierende Verschlüsselung benutzt.

Wenn sowohl SafeGuard Data Exchange als auch File Encryption auf einem Endpoint installiert ist, kann es vorkommen, dass eine SafeGuard Data Exchange Verschlüsselungsrichtlinie für ein Laufwerk auf dem Computer definiert ist und gleichzeitig File Encryption Richtlinien für Ordner auf demselben Laufwerk gelten. Ist dies der Fall, so erhält die SafeGuard Data Exchange Richtlinie Vorrang vor den **File Encryption** Richtlinien. Neue Dateien werden gemäß der SafeGuard Data Exchange Richtlinie verschlüsselt.

Weitere Informationen zu SafeGuard Data Exchange finden Sie unter SafeGuard Data Exchange (Seite 193).

24 SafeGuard Data Exchange

Mit SafeGuard Data Exchange lassen sich Daten, die auf mit Endpoint-Computern verbundenen Wechselmedien gespeichert werden, verschlüsseln und mit anderen Benutzern austauschen. Alle Ver- und Entschlüsselungsprozesse laufen transparent und mit minimaler Benutzerinteraktion ab.

Nur Benutzer, die über die entsprechenden Schlüssel verfügen, können den Inhalt der verschlüsselten Daten lesen. Alle nachfolgenden Verschlüsselungsprozesse laufen transparent.

In der zentralen Administration definieren Sie, wie Daten auf Wechselmedien behandelt werden sollen.

Als Sicherheitsbeauftragter legen Sie die spezifischen Einstellungen in einer Richtlinie vom Typ **Geräteschutz** mit **Wechselmedien** als **Ziel des Geräteschutzes** fest.

Für SafeGuard Data Exchange muss dateibasierende Verschlüsselung benutzt werden.

24.1 Gruppenschlüssel

Für den Austausch von verschlüsselten Daten zwischen Benutzern müssen SafeGuard Enterprise Gruppenschlüssel verwendet werden. Wenn sich der Gruppenschlüssel in den Schlüsselringen der Benutzer befindet, erhalten diese vollen transparenten Zugriff auf die mit ihren Computern verbundenen Wechselmedien.

Auf Computern ohne SafeGuard Enterprise ist der Zugriff auf verschlüsselte Daten auf Wechselmedien nicht möglich. Eine Ausnahme ist hier der zentrale definierte Domänen-/Gruppenschlüssel, der in Verbindung mit der Medien-Passphrase benutzt werden kann.

Hinweis: Um verschlüsselte Daten auf Wechselmedien auch auf/mit Computern ohne SafeGuard Enterprise zu benutzen/weiterzugeben, können Sie SafeGuard Portable benutzen. Für SafeGuard Portable ist die Verwendung von lokalen Schlüsseln oder einer Medien-Passphrase erforderlich.

24.2 Lokale Schlüssel

SafeGuard Data Exchange unterstützt die Verschlüsselung mit lokalen Schlüsseln. Lokale Schlüssel werden auf dem Benutzercomputer erzeugt und können zur Verschlüsselung von Wechselmedien benutzt werden. Die Schlüssel werden durch Eingabe einer Passphrase erstellt. In der SafeGuard Enterprise Datenbank wird jeweils eine Sicherungskopie des lokalen Schlüssels erstellt.

Hinweis: Ein Benutzer ist standardmäßig dazu berechtigt, lokale Schlüssel zu erzeugen. Sollen Benutzer nicht dazu berechtigt sein, so müssen Sie diese Option explizit deaktivieren. Dies muss in einer Richtlinie vom Typ **Geräteschutz** mit **Lokale Datenträger** als **Ziel des Geräteschutzes** festgelegt werden (**Allgemeine Einstellungen > Benutzer darf einen lokalen Schlüssel erzeugen > Nein**).

Werden lokale Schlüssel zum Verschlüsseln von Dateien auf Wechselmedien verwendet, lassen sich diese Dateien auf einem Computer ohne SafeGuard Data Exchange mit SafeGuard Portable entschlüsseln. Beim Öffnen der Dateien mit SafeGuard Portable wird der Benutzer dazu aufgefordert, die Passphrase einzugeben, die beim Erzeugen des Schlüssels angegeben wurde. Wenn dem Benutzer die Passphrase bekannt ist, kann er die Datei öffnen.

Mit SafeGuard Portable erhält jeder Benutzer, der die entsprechende Passphrase kennt, Zugang zu verschlüsselten Dateien auf Wechselmedien. Auf diese Weise ist ein Austausch von verschlüsselten Daten mit Partnern, die SafeGuard Enterprise nicht installiert haben, möglich. Sie benötigen lediglich SafeGuard Portable sowie die Passphrase für die Dateien, auf die sie zugreifen sollen.

Durch Verwendung von verschiedenen lokalen Schlüsseln für die Verschlüsselung von Dateien auf Wechselmedien lässt sich der Zugang zu den Dateien sogar selektiv einschränken. Zum Beispiel: Sie verschlüsseln die Dateien auf einem USB-Stick mit einem Schlüssel mit der Passphrase *mein_lokalerSchlüssel*. Für eine einzelne Datei mit dem Dateinamen *FürPartner.doc* verwenden Sie die Passphrase *partner_lokalerSchlüssel*. Wenn Sie den USB-Stick nun an einen Partner weitergeben und ihm die Passphrase *partner_lokalerSchlüssel* mitteilen, hat dieser nur Zugriff auf die Datei *FürPartner.doc.*

Hinweis: Standardmäßig wird SafeGuard Portable automatisch auf die am System angeschlossenen Wechselmedien kopiert, sobald Inhalte auf die von einer Verschlüsselungsregel abgedeckten Medien geschrieben werden. Um SafeGuard Portable nicht auf die Wechselmedien zu kopieren, deaktivieren Sie die Option **SafeGuard Portable auf das Ziel kopieren** in einer Richtlinie vom Typ **Geräteschutz**.

24.3 Medien-Passphrase

SafeGuard Data Exchange ermöglicht es Ihnen festzulegen, dass eine einzige Medien-Passphrase für alle Wechselmedien - mit Ausnahme von optischen Medien - auf den Endpoints erstellt werden muss. Die Medien-Passphrase ermöglicht sowohl den Zugriff auf alle zentral definierten Domänen-/Gruppenschlüssel als auch auf alle in SafeGuard Portable verwendeten lokalen Schlüssel. Der Benutzer muss nur eine einzige Passphrase eingeben und erhält Zugriff auf alle verschlüsselten Dateien in SafeGuard Portable. Dabei spielt es keine Rolle, welcher lokale Schlüssel für die Verschlüsselung verwendet wurde.

Auf jedem Endpoint wird automatisch ein einzigartiger Medienverschlüsselungsschlüssel für die Datenverschlüsselung für jedes Medium erstellt. Dieser Schlüssel ist durch die Medien-Passphrase und einen zentral definierten Domänen-/Gruppenschlüssel gesichert. Auf einem Computer mit SafeGuard Data Exchange ist es daher nicht notwendig, die Medien-Passphrase einzugeben, um auf die verschlüsselten Dateien auf Wechselmedien zuzugreifen. Der Zugriff wird automatisch gewährt, wenn sich der entsprechende Schlüssel im Schlüsselring des Benutzers befindet.

Der zu verwendende Domänen-/Gruppenschlüssel muss unter **Für Verschlüsselung definierter Schlüssel** festgelegt werden.

Die Medien-Passphrase-Funktionalität steht zur Verfügung, wenn die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie vom Typ **Geräteschutz** aktiviert ist.

Nach dem Wirksamwerden dieser Einstellung auf dem Endpoint wird der Benutzer automatisch aufgefordert, eine Medien-Passphrase einzugeben, wenn er zum ersten Mal Wechselmedien mit dem Computer verbindet. Die Medien-Passphrase ist auf allen Computern, auf denen sich der Benutzer anmelden darf, gültig. Der Benutzer kann die Medien-Passphrase auch ändern. In diesem Fall findet automatisch eine Synchronisierung statt, wenn die Medien-Passphrase auf dem Computer und die Medien-Passphrase der Wechselmedien nicht mehr synchron sind.

Sollte der Benutzer die Medien-Passphrase vergessen, so kann er diese ohne Helpdesk-Unterstützung wiederherstellen.

Hinweis: Um die Medien-Passphrase zu aktivieren, aktivieren Sie die Option **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen** in einer Richtlinie vom Typ

Geräteschutz. Diese Einstellung steht nur dann zur Verfügung, wenn Sie als **Ziel des Geräteschutzes** die Option **Wechselmedien** gewählt haben.

24.3.1 Medien-Passphrase und Standalone-Endpoints

Auf einem Standalone-Endpoint (d. h. auf einem Endpoint, der nicht zentral verwaltet wird) stehen ohne aktivierte Medien-Passphrase-Funktion nach der Installation keine Schlüssel zur Verfügung, da Standalone-Endpoints nur lokale Schlüssel verwenden. Vor der Benutzung der Verschlüsselung muss der Benutzer einen Schlüssel erzeugen.

Ist die Medien-Passphrase-Funktionalität in einer Wechselmedienrichtlinie für diese Endpoints aktiviert, so wird der Medienverschlüsselungsschlüssel automatisch auf dem Endpoint erzeugt und kann direkt nach Abschluss der Installation für die Verschlüsselung verwendet werden. Der Schlüssel steht als „vordefinierter“ Schlüssel im Schlüsselring des Benutzers zur Verfügung und wird in Dialogen für die Schlüsselauswahl als <Benutzername> angezeigt.

Falls verfügbar, werden die Medienverschlüsselungsschlüssel auch für alle initialen Verschlüsselungsvorgänge verwendet.

24.4 Best Practice

Dieser Abschnitt beschreibt einige typische Anwendungsfälle für SafeGuard Data Exchange und deren Umsetzung durch Erstellen der entsprechenden Richtlinien.

Bob und Alice sind zwei Mitarbeiter des gleichen Unternehmens und haben beide SafeGuard Data Exchange installiert. Joe ist ein externer Partner. Auf seinem Computer ist SafeGuard Enterprise nicht installiert.

24.4.1 Unternehmensinterne Anwendung

Bob möchte verschlüsselte Daten auf Wechselmedien an Alice weitergeben. Beide gehören derselben Gruppe an und haben daher den entsprechenden Gruppenschlüssel in ihrem SafeGuard Enterprise Schlüsselring. Da sie den Gruppenschlüssel benutzen, können sie transparent auf die verschlüsselten Dateien zugreifen, ohne eine Passphrase eingeben zu müssen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien: Dateibasierend**
- **Schlüssel für die Verschlüsselung: Definierter Schlüssel aus der Liste**
  - Definierter Schlüssel aus der Liste: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien: Ja**

  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien zum ersten Mal mit dem System verbunden werden.

- **Benutzer darf Initialverschlüsselung abbrechen: Nein**

Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.

- **Benutzer darf auf unverschlüsselte Dateien zugreifen: Nein**

  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.

- **Benutzer darf Dateien entschlüsseln: Nein**

  Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

- **SafeGuard Portable auf das Ziel kopieren: Nein**

  Für die gemeinsame Benutzung von Wechselmedien innerhalb der Arbeitsgruppe ist SafeGuard Portable nicht erforderlich. Außerdem würde SafeGuard Portable das Entschlüsseln von Dateien auf Computern ohne SafeGuard Enterprise erlauben.

Die Benutzer können Daten einfach durch Austausch von Wechselmedien gemeinsam nutzen. Wenn sie die Wechselmedien mit ihren Computern verbinden, haben sie transparenten Zugriff auf verschlüsselte Dateien.

Hinweis: Dieser Anwendungsfall kann durch Benutzung von SafeGuard Enterprise Device Encryption umgesetzt werden. Hier ist das gesamte Wechselmedium sektorbasierend verschlüsselt.

24.4.2 Anwendung bei Heimarbeit oder für persönlichen Gebrauch auf Dritt-Computern

- **Heimarbeit:**

  Bob möchte seine verschlüsselten Wechselmedien auf seinem Computer zuhause benutzen, auf dem SafeGuard Enterprise nicht installiert ist. Auf seinem Computer zuhause entschlüsselt Bob Dateien mit SafeGuard Portable. Da für alle seine Wechselmedien eine einzige Medien-Passphrase definiert ist, muss Bob nur SafeGuard Portable öffnen und die Medien-Passphrase eingeben. Danach hat Bob transparenten Zugriff auf alle verschlüsselten Dateien, unabhängig davon, welcher lokale Schüssel für die Verschlüsselung verwendet wurde.

- **Persönlicher Gebrauch auf Dritt-Computern:**

  Bob verbindet das Wechselmedium mit Joes (externer Partner) Computer und gibt die Medien-Passphrase ein, um Zugriff auf die auf dem Medium gespeicherten verschlüsselten Dateien zu erhalten. Bob kann die Dateien nun - verschlüsselt oder unverschlüsselt - auf Joes Computer kopieren.

Verhalten auf dem Endpoint:

- Bob verbindet das Wechselmedium zum ersten Mal mit dem Computer.
- Der Medienverschlüsselungsschlüssel, der für jedes Medium einzigartig ist, wird automatisch erzeugt.
- Bob wird aufgefordert, die Medien-Passphrase für die Offline-Nutzung über SafeGuard Portable einzugeben.
- Der Benutzer muss nichts über den zu verwendenden Schlüssel oder den Schlüsselring wissen. Der Medienverschlüsselungsschlüssel wird ohne Benutzerinteraktion immer für

die Datenverschlüsselung verwendet. Der Medienverschlüsselungsschlüssel ist für den Benutzer auch nicht sichtbar. Nur der zentral definierte Gruppen-/Domänenschlüssel ist sichtbar.

- Bob und Alice haben innerhalb der gleichen Gruppe oder Domäne transparenten Zugriff, da sie beide den gleichen Gruppen-/Domänenschlüssel verwenden.
- Wenn Bob auf verschlüsselte Dateien auf Wechselmedien auf einem Computer ohne SafeGuard Data Exchange zugreifen möchte, kann er die Medien-Passphrase in SafeGuard Portable benutzen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien: Dateibasierend**
- **Schlüssel für die Verschlüsselung: Definierter Schlüssel aus der Liste**

  Definierter Schlüssel aus der Liste: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen.

- **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen: Ja**

  Der Benutzer definiert eine Medien-Passphrase auf seinem Computer, die für alle seine Wechselmedien gilt.

- **SafeGuard Portable auf das Ziel kopieren: Ja**

  SafeGuard Portable gibt dem Benutzer in einem System ohne SafeGuard Data Exchange Zugriff auf alle verschlüsselten Dateien auf den Wechselmedien durch die Eingabe einer einzigen Medien-Passphrase.

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien: Ja**

  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien zum ersten Mal mit dem System verbunden werden.

- **Benutzer darf Initialverschlüsselung abbrechen: Nein**

  Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.

- **Benutzer darf auf unverschlüsselte Dateien zugreifen: Nein**

  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.

- **Benutzer darf Dateien entschlüsseln: Nein**

  Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

Im Büro haben sowohl Bob als auch Alice transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause oder auf Dritt-Computern können sie verschlüsselte Dateien mit SafeGuard Portable öffnen. Die Benutzer müssen nur die Medien-Passphrase eingeben und erhalten somit Zugriff auf alle verschlüsselten Dateien. Dies ist eine einfache und sichere Methode für die Verschlüsselung von Daten auf allen Wechselmedien. Ziel dieser Konfiguration

ist es, die Benutzerinteraktion auf ein Minimum zu reduzieren und trotzdem jede Datei auf Wechselmedien zu verschlüsseln und den Benutzern Zugriff auf die verschlüsselten Dateien im Offline-Modus zu geben. Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

Hinweis: In dieser Konfiguration sind Benutzer nicht dazu berechtigt, lokale Schlüssel zu erzeugen, da dies in diesem Anwendungsfall nicht notwendig ist. Dies muss in einer Richtlinie vom Typ **Geräteschutz** mit **Lokale Datenträger** als Ziel des Geräteschutzes festgelegt werden (**Allgemeine Einstellungen > Benutzer darf einen lokalen Schlüssel erzeugen > Nein**).

- **SafeGuard Portable auf Wechselmedien kopieren: Nr.**

  Für die gemeinsame Benutzung von Wechselmedien innerhalb der Arbeitsgruppe ist SafeGuard Portable nicht erforderlich. Außerdem würde SafeGuard Portable das Entschlüsseln von Dateien auf Computern ohne SafeGuard Enterprise erlauben.

Im Büro haben die Benutzer transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause öffnen sie verschlüsselte Dateien mit SafeGuard Portable. Die Benutzer müssen nur die Medien-Passphrase eingeben und erhalten somit Zugriff auf alle verschlüsselten Dateien, unabhängig davon, welcher Schlüssel für die Verschlüsselung verwendet wurde.

24.4.3 Weitergabe von Wechselmedien an externe Partner

Hinweis: Dieses Beispiel gilt nur für Windows Endpoints.

Bob möchte ein verschlüsseltes Medium an Joe (externer Partner) weitergeben, der SafeGuard Data Exchange nicht installiert hat und daher SafeGuard Portable verwenden muss. Bob möchte Joe jedoch nicht auf alle verschlüsselten Dateien auf dem Wechselmedium Zugriff geben. Er kann hierzu einen lokalen Schlüssel erzeugen und die Dateien mit dem lokalen Schlüssel verschlüsseln. Joe kann nun mit SafeGuard Portable die verschlüsselten Dateien mit der Passphrase des lokalen Schlüssels öffnen. Bob dagegen kann immer noch die Medien-Passphrase für den Zugriff auf alle Dateien auf dem Wechselmedium benutzen.

Verhalten auf dem Computer:

- Bob verbindet das Wechselmedium zum ersten Mal mit dem Computer. Der Medienverschlüsselungsschlüssel, der für jedes Medium einzigartig ist, wird automatisch erzeugt.
- Bob wird aufgefordert, die Medien-Passphrase für die Offline-Nutzung einzugeben.
- Der Medienverschlüsselungsschlüssel wird ohne Benutzerinteraktion für die Datenverschlüsselung verwendet, aber...
- Bob kann nun einen lokalen Schlüssel (z. B. mit der Bezeichnung JoeSchlüssel) für die Verschlüsselung der spezifischen Dateien, die mit Joe ausgetauscht werden sollen, erzeugen oder auswählen.
- Bob und Alice haben innerhalb der gleichen Gruppe oder Domäne transparenten Zugriff, da sie beide den gleichen Gruppen-/Domänenschlüssel verwenden.
- Wenn Bob auf verschlüsselte Dateien auf Wechselmedien auf einem Computer ohne SafeGuard Data Exchange zugreifen möchte, kann er die Medien-Passphrase in SafeGuard Portable benutzen.

- Joe kann auf die spezifischen Dateien durch Eingabe der Passphrase des Schlüssels JoeSchlüssel zugreifen, ohne auf die restlichen Dateien auf dem Wechselmedium zugreifen zu müssen.

Die notwendigen Einstellungen legen Sie in einer Richtlinie vom Typ **Geräteschutz\Wechselmedien** fest:

- **Verschlüsselungsmodus für Medien: Dateibasierend**

- **Schlüssel für die Verschlüsselung: Beliebiger Schlüssel im Schlüsselring des Benutzers**

  Ermöglicht dem Benutzer die Auswahl unterschiedlicher Schlüssel für die Verschlüsselung von Dateien auf Wechselmedien.

  Für Verschlüsselung definierter Schlüssel: <Gruppen-/Domänenschlüssel> (z. B. group_users_Bob_Alice@DC=...), um sicherzustellen, dass beide denselben Schlüssel benutzen und um beiden den transparenten Zugriff auf Wechselmedien zu ermöglichen, wenn sie sie mit ihren Computern im Büro verbinden.

- **Benutzer darf eine Medien-Passphrase für Wechselmedien erzeugen: Ja**

  Der Benutzer definiert eine Medien-Passphrase auf seinem Computer, die für alle seine Wechselmedien gilt.

- **SafeGuard Portable auf das Ziel kopieren: Ja**

  SafeGuard Portable gibt dem Benutzer in einem System ohne SafeGuard Data Exchange Zugriff auf alle verschlüsselten Dateien auf den Wechselmedien durch die Eingabe einer einzigen Medien-Passphrase.

Wenn die Firmenrichtlinien zusätzlich festlegen, dass alle Dateien auf Wechselmedien immer verschlüsselt werden sollen, fügen Sie folgende Einstellungen hinzu:

- **Initialverschlüsselung aller Dateien: Ja**

  Stellt sicher, dass Dateien auf Wechselmedien verschlüsselt werden, sobald die Wechselmedien zum ersten Mal mit dem System verbunden werden.

- **Benutzer darf Initialverschlüsselung abbrechen: Nein**

  Der Benutzer kann die Initialverschlüsselung nicht abbrechen, um sie z. B. zu einem späteren Zeitpunkt durchzuführen.

- **Benutzer darf auf unverschlüsselte Dateien zugreifen: Nein**

  Werden auf Wechselmedien unverschlüsselte Dateien entdeckt, so wird der Zugriff auf diese Dateien verweigert.

- **Benutzer darf Dateien entschlüsseln: Nein**

  Der Benutzer darf Dateien auf Wechselmedien nicht entschlüsseln.

Im Büro haben sowohl Bob als auch Alice transparenten Zugriff auf verschlüsselte Dateien auf Wechselmedien. Zuhause können sie verschlüsselte Dateien mit SafeGuard Portable durch Eingabe der Medien-Passphrase öffnen. Wenn Bob oder Alice die Wechselmedien an einen Dritt-Computer weitergeben möchten, auf dem SafeGuard Data Exchange nicht installiert ist, können sie mit lokalen Schlüsseln sicherstellen, dass externe Partner nur auf einige spezifische Dateien zugreifen können. Dies ist eine erweiterte Konfiguration, die durch die Möglichkeit, lokale Schlüssel auf den Computern zu erzeugen, ein höheres Maß an Benutzerinteraktion umfasst.

Hinweis: Voraussetzung für diesen Beispielanwendungsfall ist es, dass der Benutzer dazu berechtigt ist, lokale Schlüssel zu erzeugen (Standardeinstellung in SafeGuard Enterprise).

24.5 Konfigurieren von vertrauenswürdigen und ignorierten Anwendungen für SafeGuard Data Exchange

Sie können Anwendungen als vertrauenswürdig definieren, um ihnen Zugriff auf verschlüsselte Dateien zu geben. Dies ist zum Beispiel notwendig, damit Antivirus-Software verschlüsselte Dateien überprüfen kann.

Sie können Anwendungen als ignoriert definieren, um sie von der transparenten Dateiverschlüsselung/Dateientschlüsselung auszuschließen. Wenn Sie zum Beispiel ein Backup-Programm als ignorierte Anwendung definieren, bleiben die vom Programm gesicherten verschlüsselten Daten verschlüsselt.

Hinweis: Untergeordnete Prozesse werden nicht als vertrauenswürdig/ignoriert eingestuft.

1. Legen Sie im **Richtlinien** Navigationsbereich einen neue Richtlinie vom Typ **Allgemeine Einstellungen** an oder wählen Sie eine vorhandene aus.
2. Klicken Sie unter **Dateiverschlüsselung** auf die Dropdown-Schaltfläche der Felder **Vertrauenswürdige Anwendungen** oder **Ignorierte Anwendungen**.
3. Geben Sie im Editor-Listenfeld die Anwendungen ein, die Sie als vertrauenswürdig/ignoriert definieren möchten.
   - Sie können mehrere vertrauenswürdige/ignorierte Anwendungen in einer Richtlinie definieren. Jede Zeile im Editor-Listenfeld definiert jeweils eine Anwendung.
   - Anwendungsnamen müssen auf .exe enden.
   - Anwendungsnamen müssen als Fully Qualified Paths mit Laufwerk/Verzeichnis definiert werden. Es reicht nicht aus, nur den Dateinamen einzugeben (zum Beispiel "beispiel.exe"). Aus Gründen der Benutzerfreundlichkeit zeigt die Einzelzeilenansicht der Anwendungsliste nur die Dateinamen getrennt durch Strichpunkte.
4. Speichern Sie Ihre Änderungen.

Hinweis: Die Richtlinieneinstellungen **Vertrauenswürdige Anwendungen** und **Ignorierte Anwendungen** sind Computereinstellungen. Die Richtlinie muss daher Computern, nicht Benutzern, zugewiesen werden. Andernfalls werden die Einstellungen nicht wirksam.

24.6 Konfigurieren von ignorierten Geräten für SafeGuard Data Exchange

Sie können Geräte als ignoriert definieren, um sie von der Dateiverschlüsselung auszuschließen. Sie können nur vollständige Geräte ausschließen.

1. Legen Sie im **Richtlinien** Navigationsbereich einen neue Richtlinie vom Typ **Allgemeine Einstellungen** an oder wählen Sie eine vorhandene aus.
2. Klicken Sie unter **Dateiverschlüsselung** auf die Dropdown-Schaltfläche des Felds **Ignorierte Geräte**.

3. Geben Sie die entsprechenden Gerätenamen ein, um spezifische Geräte von der Verschlüsselung auszuschließen. Dies ist zum Beispiel nützlich, wenn Sie Systeme von Dritt-Anbietern ausschließen müssen.

   Hinweis: Sie können die Namen der derzeit im System benutzten Geräte mit Tools von Dritt-Anbietern (z. B. OSR Device Tree) anzeigen lassen. SafeGuard Enterprise protokolliert alle Geräte, mit denen eine Verbindung hergestellt wird. Mit Hilfe von Registry Keys können Sie eine Liste von verbundenen und ignorierten Geräten aufrufen.

24.6.1 Anzeige von verbundenen und ignorierten Geräten für die SafeGuard Data Exchange Konfiguration

Als Hilfestellung für die Definition von ignorierten Geräten können Sie mit Registry Keys ermitteln, welche Geräte für die Verschlüsselung in Betracht gezogen werden (verbundene Geräte) und welche Geräte derzeit ignoriert werden. Die Liste mit ignorierten Geräten enthält nur Geräte, die tatsächlich auf dem Computer verfügbar sind und ignoriert werden. Wird ein Gerät in einer Richtlinie als ignoriert definiert und das Gerät ist nicht verfügbar, so wird das Gerät auch nicht aufgelistet.

Benutzen Sie folgende Registry Keys, um verbundene und ignorierte Geräte zu ermitteln:

- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\AttachedDevices`**
- **`HKLM\System\CurrentControlSet\Control\Utimaco\SGLCENC\Log\IgnoredDevices`**

24.7 Konfigurieren der persistenten Verschlüsselung für SafeGuard Data Exchange

Der Inhalt von mit SafeGuard Data Exchange verschlüsselten Dateien wird jeweils direkt entschlüsselt, wenn der Benutzer den erforderlichen Schlüssel hat. Wenn der Inhalt in einer neuen Datei an einem Ablageort gespeichert wird, für den keine Verschlüsselungsregel gilt, bleibt die resultierende neue Datei unverschlüsselt.

Mit persistenter Verschlüsselung bleiben Kopien von verschlüsselten Dateien auch dann verschlüsselt, wenn sie an einem Speicherort abgelegt werden, für den keine Verschlüsselungsregel gilt.

Sie können die persistente Verschlüsselung in Richtlinien vom Typ **Allgemeine Einstellungen** konfigurieren. Die Richtlinieneinstellung **Persistente Verschlüsselung aktivieren** ist standardmäßig aktiviert.

Hinweis:

- Wenn Dateien an ein ignoriertes Gerät oder in einen Ordner kopiert oder verschoben werden, für den eine Richtlinie mit dem **Modus** für die Verschlüsselung **Ignorieren** gilt, hat die Einstellung **Persistente Verschlüsselung aktivieren** keine Auswirkungen.
- Kopiervorgänge werden anhand des Dateinamens erkannt. Wenn ein Benutzer eine verschlüsselte Datei mit **Speichern unter** unter einem anderen Dateinamen an einem Speicherort speichert, für den keine Verschlüsselungsregel gilt, ist die Datei unverschlüsselt.

24.8 Protokollierung des Dateizugriffs auf Wechselmedien

Mit der Funktion **Berichte** des SafeGuard Management Center lässt sich der Dateizugriff auf Wechselmedien protokollieren (Datei-Tracking). Für Datei-Tracking spielt es keine Rolle, ob für Dateien auf Wechselmedien eine Verschlüsselungsrichtlinie gilt.

In einer Richtlinie vom Typ **Protokollierung** können Sie Folgendes konfigurieren:

- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis auf dem Wechselmedium angelegt wird.
- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis auf dem Wechselmedium umbenannt wird.
- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis vom Wechselmedium gelöscht wird.

Weitere Informationen finden Sie unter Datei-Tracking-Bericht für Wechselmedien und Cloud-Speicher (Seite 275).

24.9 SafeGuard Data Exchange und File Encryption

Das SafeGuard Enterprise Modul File Encryption bietet dateibasierende Verschlüsselung im Netzwerk, speziell für Arbeitsgruppen bei Netzwerkfreigaben.

Wenn sowohl SafeGuard Data Exchange als auch File Encryption auf einem Endpoint installiert ist, kann es vorkommen, dass eine SafeGuard Data Exchange Verschlüsselungsrichtlinie für ein Laufwerk auf dem Computer definiert ist und gleichzeitig File Encryption Richtlinien für Ordner auf demselben Laufwerk gelten. Ist dies der Fall, so erhält die SafeGuard Data Exchange Richtlinie Vorrang vor den File Encryption Richtlinien. Neue Dateien werden gemäß der SafeGuard Data Exchange Richtlinie verschlüsselt.

Weitere Informationen finden Sie unter Dateiverschlüsselung (Seite 181).

25 Cloud Storage

Das SafeGuard Enterprise Modul Cloud Storage bietet dateibasierende Verschlüsselung von in der Cloud gespeicherten Daten.

Das Modul beeinflusst nicht die Art und Weise, wie Benutzer mit in der Cloud gespeicherten Daten arbeiten. Die Benutzer verwenden weiterhin die anbieterspezifischen Synchronisationsapplikationen zum Übertragen von Daten an die Cloud und Empfangen von Daten aus der Cloud. Das Modul Cloud Storage stellt sicher, dass die lokalen Kopien der in der Cloud gespeicherten Daten transparent verschlüsselt werden. Sie werden somit immer in verschlüsselter Form in der Cloud gespeichert.

Für Cloud Storage legen Sie im SafeGuard Management Center **Cloud Storage Definitionen** an und verwenden diese als Ziel für Richtlinien vom Typ **Geräteschutz**. Es stehen für mehrere Cloud Storage Anbieter, zum Beispiel Dropbox oder Egnyte, vordefinierte Cloud Storage Definitionen zur Verfügung.

Wenn für Endpoints eine Cloud Storage Richtlinie gilt, werden die Dateien in den von der Richtlinie abgedeckten Speicherorten ohne Benutzerinteraktion transparent verschlüsselt:

- Verschlüsselte Dateien werden an die Cloud synchronisiert.
- Aus der Cloud erhaltene verschlüsselte Dateien können wie üblich mit Applikationen modifiziert werden.

Mit SafeGuard Portable kann auf durch Cloud Storage verschlüsselte Dateien auf Endpoints ohne SafeGuard Enterprise Cloud Storage zugegriffen werden. Verschlüsselte Dateien können so auch in diesem Fall gelesen werden.

Hinweis: Cloud Storage verschlüsselt nur neue in der Cloud gespeicherte Daten. Wurden Daten bereits vor der Installation des Moduls Cloud Storage in der Cloud gespeichert, so werden diese Daten nicht automatisch verschlüsselt. Wenn Sie solche Daten verschlüsseln möchten, müssen Sie sie zunächst aus der Cloud entfernen und dann wieder einfügen.

25.1 Anforderungen für Software von Cloud Storage Anbietern

Damit die Verschlüsselung für in der Cloud gespeicherten Daten möglich ist, muss die Software des Cloud Storage Anbieters

- auf dem Computer, auf dem das Modul Cloud Storage installiert ist, laufen.
- eine Anwendung (oder einen Systemdienst) im lokalen Dateisystem für die Synchronisierung zwischen der Cloud und dem lokalen System enthalten.
- die synchronisierten Daten im lokalen Dateisystem speichern.

25.2 Anlegen von Cloud Storage Definitionen

Im SafeGuard Management Center stehen für mehrere Cloud Storage Anbieter, zum Beispiel Dropbox oder Egnyte, vordefinierte Cloud Storage Definitionen zur Verfügung. Sie können die in den vordefinierten Cloud Storage Definitionen festgelegten Pfade nach Ihren Anforderungen ändern oder eine neue Cloud Storage Definition erstellen und Werte aus der vordefinierten als Grundlage kopieren. Dies ist vor allem dann hilfreich, wenn Sie nur einen

Teil der Daten in der Cloud Storage verschlüsseln möchten. Sie können auch eigene Cloud Storage Definitionen anlegen.

Hinweis: Wenn bestimmte Ordner verschlüsselt werden (zum Beispiel der Dropbox Installationsordner), bewirkt dies unter Umständen, dass das Betriebssystem oder bestimmte Anwendungen nicht mehr laufen. Stellen Sie beim Anlegen von Cloud Storage Definitionen für **Geräteschutz** Richtlinien sicher, dass diese Ordner nicht verschlüsselt werden.

1. Wählen Sie im **Richtlinien** Navigationsbereich **Cloud Storage Definitionen**.
2. Klicken Sie im Kontextmenü von **Cloud Storage Definitionen** auf **Neu > Cloud Storage Definition**.
3. Der **Neue Cloud Storage Definition** Dialog wird angezeigt. Geben Sie einen Namen für die Cloud Storage Definition ein.
4. Klicken Sie auf **OK**. Die Cloud Storage Definition wird mit dem eingegebenen Namen unter dem Stammknoten **Cloud Storage Definitionen** im **Richtlinien** Navigationsbereich angezeigt.
5. Wählen Sie die Cloud Storage Definition aus. Im Arbeitsbereich auf der rechten Seite wird der Inhalt der Cloud Storage Definition angezeigt:

   - **Name des Ziels:**

     Der zu Beginn eingegebene Name. Dieser wird zur Referenzierung der Cloud Storage Definition als Ziel für eine Richtlinie des Typs **Geräteschutz** benutzt.
   - **Synchronisierungsapplikation:**

     Geben Sie den Pfad und die Anwendung für die Synchronisierung der Daten mit der Cloud ein (zum Beispiel: <Desktop>\dropbox\dropbox.exe). Die Applikation muss sich auf einem lokalen Laufwerk befinden.
   - **Synchronisierungsordner:**

     Geben Sie den/die Ordner ein, der/die mit der Cloud synchronisiert wird/werden. Es werden nur lokale Pfade unterstützt.

     Hinweis: Für Pfade in den Einstellungen **Synchronisierungsapplikation** und **Synchronisierungsordner** werden die gleichen Platzhalter wie für **File Encryption** unterstützt (siehe Platzhalter für Pfade in File Encryption Verschlüsselungsregeln (Seite 185)).

25.2.1 Platzhalter für Cloud Storage Anbieter

Als Sicherheitsbeauftragter können Sie Platzhalter für Cloud Storage Anbieter verwenden, um Synchronisierungsapplikationen und Synchronisierungsordner zu definieren. Diese Platzhalter stehen für unterstützte Cloud Storage Applikationen von Drittanbietern. Mit den Platzhaltern können Sie eine bestimmte Applikation eines Drittanbieters angeben und denselben Platzhalter zum Verweis auf die Synchronisierungsordner verwenden, die von der Applikation zur Synchronisierung verwendet werden.

Platzhalter für Cloud Storage Anbieter werden zwischen <! und !> gesetzt.

Hinweis: SafeGuard Enterprise Version 7.0 unterstützt Dropbox und Google Drive für OS X endpoints.

Derzeit unterstützte Platzhalter

<table>
<tr><th>Anbieter</th><th>Platzhalter</th><th>Kann in CSD-Einstellung verwendet werden.</th><th>Wird aufgelöst in</th></tr>
<tr><td>Dropbox</td><td><!Dropbox!></td><td>Synchronisierungsapplikation, Synchronisierungsordner</td><td>Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der Dropbox-Software benutzt wird.

Für Synchronisierungsordner: Der "Fully qualified"-Pfad des Synchronisierungsordners, der von der Dropbox-Software benutzt wird.</td></tr>
<tr><td rowspan="4">Egnyte</td><td><!Egnyte!></td><td>Synchronisierungsapplikation</td><td>Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der Egnyte-Software benutzt wird.</td></tr>
<tr><td><!EgnytePrivate!></td><td>Synchronisierungsordner</td><td>Alle privaten Ordner in der Egnyte Cloud Storage. Für Standard-Egnyte-Benutzer ist dies in der Regel ein einzelner Ordner. Für Egnyte-Administratoren, wird dieser Platzhalter in der Regel in mehrere Ordner umgesetzt.</td></tr>
<tr><td><!EgnyteShared!></td><td>Synchronisierungsordner</td><td>Alle freigegebenen Ordner in der Egnyte Cloud Storage.</td></tr>
<tr><td colspan="3">Hinweis:

Änderungen an der Egnyte-Ordnerstruktur (auch das Hinzufügen oder Entfernen von privaten oder freigegebenen Ordnern) werden automatisch erkannt. Die entsprechenden Richtlinien werden automatisch angepasst.

Hinweis: Da sich Egnyte-Synchronisierungsordner im Netzwerk befinden können, können Sie bei der Einstellung Synchronisierungsordner Netzwerkpfade eingeben.</td></tr>
</table>

<table>
<tr><th>Anbieter</th><th>Platzhalter</th><th>Kann in CSD-Einstellung verwendet werden.</th><th>Wird aufgelöst in</th></tr>
<tr><td></td><td colspan="3">Das SafeGuard Enterprise Cloud Storage Modile verbindet sich daher standardmäßig mit Netzwerkdateisystemen. Wenn dies nicht erforderlich ist, können Sie dieses Verhalten deaktivieren, indem Sie eine Richtlinie vom Typ Allgemeine Einstellungen definieren und unter Ignorierte Geräte die Option Netzwerk auswählen.</td></tr>
<tr><td>Google Drive</td><td><code><!GoogleDrive!></code></td><td>Synchronisierungsapplikation, Synchronisierungsordner</td><td>Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der Google Drive Software benutzt wird.

Für Synchronisierungsordner: Der "Fully qualified"-Pfad des Synchronisierungsordners, der von der Google Drive Software benutzt wird.</td></tr>
<tr><td rowspan="2">OneDrive</td><td><code><!OneDrive!></code></td><td>Synchronisierungsapplikation, Synchronisierungsordner</td><td>Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der OneDrive-Software benutzt wird.

Für Synchronisierungsordner: Der "Fully qualified"-Pfad der Synchronisierungsordner, die von der OneDrive-Software benutzt werden.</td></tr>
<tr><td colspan="3">Hinweis: SafeGuard Enterprise unterstützt keine Microsoft Konten. Unter Windows 8.1 kann OneDrive nur benutzt werden, wenn der Windows Benutzer ein Domänenbenutzer ist. SafeGuard Enterprise unterstützt unter Windows 8.1 OneDrive nicht für lokale Benutzer.</td></tr>
<tr><td>OneDrive for Business</td><td><code><!OneDriveForBusiness!></code></td><td>Synchronisierungsapplikation, Synchronisierungsordner</td><td>Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der</td></tr>
</table>

Anbieter	Platzhalter	Kann in CSD-Einstellung verwendet werden.	Wird aufgelöst in
			OneDrive-Software benutzt wird. Für Synchronisierungsordner: Der "Fully qualified"-Pfad der Synchronisierungsordner, die von der OneDrive-Software benutzt werden.
	Hinweis: OneDrive for Business unterstützt nur das Speichern von verschlüsselten Dateien in lokalen Ordnern und ihre Synchronisierung mit der Cloud. Die Speicherung von verschlüsselten Dateien von Microsoft Office 2013 Applikationen direkt in der OneDrive for Business-Cloud oder direkt am SharePoint Server wird nicht unterstützt. Diese Dateien werden unverschlüsselt in der Cloud gespeichert. Von SafeGuard Enterprise in der OneDrive for Business-Cloud verschlüsselte Dateien können nicht von Microsoft Office 365 geöffnet werden.		
SkyDrive	**`<!SkyDrive!>`**	**Synchronisierungsapplikation, Synchronisierungsordner**	Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation, die von der OneDrive-Software benutzt wird. Für Synchronisierungsordner: Der "Fully qualified"-Pfad der Synchronisierungsordner, die von der OneDrive-Software benutzt werden.
	Da Microsoft SkyDrive auf OneDrive umbenannt hat, ist der **`<!SkyDrive!>`** Platzhalter immer noch verfügbar. Auf diese Weise können ältere Richtlinien und SafeGuard Enterprise Endpoints vor Version 7, die den **`<!OneDrive!>`** Platzhalter nicht handhaben können, ohne Änderungen verwendet werden. SafeGuard Enterprise Endpoints Version 7 können beide Platzhalter handhaben.		
Media Center	**`<!Mediacenter!>`**	**Synchronisierungsapplikation, Synchronisierungsordner**	Für Synchronisierungsapplikationen: Der "Fully qualified"-Pfad der Synchronisierungsapplikation,

Anbieter	Platzhalter	Kann in CSD-Einstellung verwendet werden.	Wird aufgelöst in
			die von der Media Center Software benutzt wird. Für Synchronisierungsordner: Der "Fully qualified"-Pfad des Synchronisierungsordners, der von der Media Center Software benutzt wird.

Beispiel

Wenn Sie Dropbox als Cloud Storage Anbieter nutzen, können Sie für die **Synchronisierungsapplikation** einfach **<!Dropbox!>** eingeben. Wenn Sie den Synchronisierungsordner nicht explizit angeben, wird <!Dropbox!> auch in die Liste mit Ordnern unter **Synchronisierungsordner** kopiert.

In diesem Beispiel wird davon ausgegangen, dass

- Sie die <!Dropbox!> für die Synchronisierungsapplikation und <!Dropbox!>\encrypt für den Synchronisierungsordner in der Cloud Storage Definition verwendet haben,
- Dropbox auf dem Endpoint installiert ist
- Der Benutzer :\dropbox als Ordner, der mit Dropbox synchronisiert werden soll, konfiguriert hat.

Wenn der durch SafeGuard Enterprise geschützte Endpoint eine Richtlinie mit einer solchen Cloud Storage Definition (CSD) erhält, werden die Platzhalter in der CSD automatisch entsprechend dem Pfad der Dropbox.exe für die Synchronisierungsapplikation umgesetzt. Außerdem wird die Dropbox-Konfiguration gelesen und die Verschlüsselungsrichtlinie auf den Ordner d:\dropbox\encrypt eingestellt.

25.2.2 Exportieren und Importieren von Cloud Storage Definitionen

Als Sicherheitsbeauftragter können Sie Cloud Storage Definitionen exportieren und importieren. Eine Cloud Storage Definition wird als .xml-Datei exportiert.

- Um eine Cloud Storage Definition zu exportieren, wählen Sie im Kontextmenü der gewünschten Cloud Storage Definition im Bereich **Richtlinie** den Befehl **Cloud Storage Definition exportieren**.

- Um eine Cloud Storage Definition zu importieren, wählen Sie im Kontextmenü des Cloud Storage Definition Knotens im Bereich **Richtlinie** den Befehl **Cloud Storage Definition importieren**.

Beide Befehle sind auch im Menü **Aktionen** des SafeGuard Management Center verfügbar.

25.3 Erstellen einer Geräteschutz-Richtlinie mit dem Ziel Cloud Storage

Die Cloud Storage Definitionen müssen bereits angelegt worden sein. Es stehen für mehrere Cloud Storage Anbieter, zum Beispiel Dropbox oder Egnyte, vordefinierte Cloud Storage Definitionen zur Verfügung.

Die Einstellungen für die Verschlüsselung von Cloud Storage Daten legen Sie in einer Richtlinie vom Typ **Geräteschutz** fest.

1. Erstellen Sie im **Richtlinien** Navigationsbereich eine neue Richtlinie vom Typ **Geräteschutz**.
2. Wählen eine Cloud Storage Definition als Ziel aus.
3. Klicken Sie auf **OK**. Die neu angelegte Richtlinie wird im Navigationsfenster unter **Richtlinien** angezeigt. Im Aktionsbereich werden alle Einstellungen für die Richtlinie vom Typ **Geräteschutz**angezeigt. Die Einstellungen können dort geändert werden.
4. Wählen Sie für die Option **Verschlüsselungsmodus für Medien** die Einstellung **Dateibasierend**. Volume-basierende Verschlüsselung wird nicht unterstützt.
5. Wählen Sie unter **Algorithmus für die Verschlüsselung** den Algorithmus, der für die Verschlüsselung der Daten in den Synchronisierungsordnern, die in der Cloud Storage Definition definiert sind, verwendet werden soll.
6. Mit den Einstellungen **Schlüssel für die Verschlüsselung** und **Für Verschlüsselung definierter Schlüssel** definieren Sie den Schlüssel oder die Schlüssel, die für die Verschlüsselung verwendet werden sollen. Weitere Informationen finden Sie unter Geräteschutz (Seite 150).
7. Wenn Sie die Einstellung **SafeGuard Portable auf das Ziel kopieren** aktivieren, wird SafeGuard Portable in jeden Synchronisierungsordner kopiert, sobald Inhalte in den Ordner geschrieben werden. SafeGuard Portable ist eine Anwendung, mit der verschlüsselte Dateien auf Windows-Computern, auf denen SafeGuard Enterprise installiert ist.

   Hinweis: Um verschlüsselte Daten, die in der Cloud gespeichert sind, mit Benutzern zu teilen, die SafeGuard Enterprise nicht installiert haben, sollten die Benutzer zum Erzeugen lokaler Schlüssel berechtigt sein (siehe Lokale Schlüssel (Seite 193)).

8. Mit der Option **Klartext-Ordner** können Sie einen Ordner definieren, der von der Verschlüsselung ausgeschlossen wird. Daten in Unterordnern des definierten Klartext-Ordners werden ebenfalls von der Verschlüsselung ausgeschlossen. SafeGuard Cloud Storage erstellt automatisch leere Klartext-Ordner in allen in der **Cloud Storage Definition** definierten Synchronisierungsordnern.

25.4 Protokollierung des Dateizugriffs im Cloud-Speicher

Mit der Funktion **Berichte** im SafeGuard Management Center lässt sich der Dateizugriff im Cloud-Speicher protokollieren (Datei-Tracking). Für Datei-Tracking spielt es keine Rolle, ob für die Dateien eine Verschlüsselungsrichtlinie gilt.

In einer Richtlinie vom Typ **Protokollierung** können Sie Folgendes konfigurieren:

- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis auf einem Wechselmedium angelegt wird.
- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis auf einem Wechselmedium umbenannt wird.

- Protokollierung eines Ereignisses, wenn eine Datei oder ein Verzeichnis auf einem Wechselmedium gelöscht wird.

Weitere Informationen finden Sie unter Datei-Tracking-Bericht für Wechselmedien und Cloud-Speicher (Seite 275).

26 Benutzer-Computer Zuordnung (UMA)

SafeGuard Enterprise verwaltet die Informationen, welcher Benutzer sich an welchem Computer anmelden darf, in einer Liste, für die der Begriff UMA (User Machine Assignment bzw. Benutzer-Computer Zuordnung) verwendet wird.

Voraussetzung für die Aufnahme in die UMA ist, dass sich der Benutzer einmal an einem Computer mit installiertem SafeGuard Enterprise angemeldet hat und als „kompletter“ Benutzer, im Sinne von SafeGuard Enterprise, im SafeGuard Management Center vorhanden ist. Als „komplett“ wird ein Benutzer dann bezeichnet, wenn für ihn nach der ersten Anmeldung ein Zertifikat erzeugt und danach sein Schlüsselring aufgebaut wurde. Erst dann ist die Möglichkeit gegeben, dass diese Benutzerdaten auch auf andere Computer repliziert werden können. Nach der Replikation kann sich der Benutzer auch auf diesen Computern in der SafeGuard POA anmelden.

In der Standardeinstellung wird der erste Benutzer, der sich nach der Installation von SafeGuard Enterprise an den Computer anmeldet, in der UMA als Besitzer dieses Computers eingetragen.

Dieses Attribut erlaubt es dem Benutzer, nachdem er sich im Rahmen der SafeGuard Power-on Authentication authentisiert hat, weiteren Benutzern die Anmeldung an diesem Computer zu ermöglichen (siehe Registrieren weiterer SafeGuard Enterprise-Benutzer (Seite 106)). Dadurch werden auch sie in die UMA für diesen Computer aufgenommen.

So wird automatisch eine Liste aufgebaut, die bestimmt, welcher Benutzer sich an welchem Computer anmelden darf. Diese Liste kann im SafeGuard Management Center bearbeitet werden.

26.1 Benutzer-Computer Zuordnung (UMA) im SafeGuard Management Center

Im SafeGuard Management Center kann eine Zuordnung von Benutzern zu bestimmten Computern vorgenommen werden. Wird ein Benutzer im SafeGuard Management Center einem Computer zugeordnet (oder umgekehrt), wird diese Zuweisung in die UMA aufgenommen. Seine Benutzerdaten (Zertifikat, Schlüssel usw.) werden auf diesen Rechner repliziert, und er kann sich an diesen Computer anmelden. Wenn ein Benutzer aus der UMA entfernt wird, werden alle Benutzerdaten automatisch aus der SafeGuard POA gelöscht. Der Benutzer kann sich dann nicht mehr an der SafeGuard POA mit Benutzername und Kennwort anmelden.

Hinweis: Um die Benutzer und Computer Zuordnung unter **Benutzer & Computer** einzusehen, benötigen Sie mindestens das Zugriffsrecht **Schreibgeschützt** für eines der beteiligten Objekte (Benutzer oder Computer). Um die Zuweisung zu definieren oder zu ändern, benötigen Sie das Zugriffsrecht **Voller Zugriff** für beide beteiligten Objekte. Die UMA-Anzeige zeigt die verfügbaren Benutzer/Maschinen gefiltert nach Ihren Zugriffsrechten. In der UMA-Anzeige, die die Computern zugewiesenen Benutzer und umgekehrt zeigt, werden Objekte, für die Sie nicht die erforderlichen Zugriffsrechte haben, zu Ihrer Information angezeigt. Sie können die Zuordnung jedoch nicht ändern.

Im Rahmen dieser Zuordnung kann auch festgelegt bzw. geändert werden, wem es erlaubt ist, weiteren Benutzern die Anmeldung an diesen Computer zu ermöglichen.

Unter **Typ** wird im SafeGuard Management Center angezeigt, wie der Benutzer in die SafeGuard Enterprise Datenbank aufgenommen wurde. **Übernommen** gibt an, dass der Benutzer auf einem Endpoint in die UMA für den Computer aufgenommen worden ist.

Hinweis: Wird im SafeGuard Management Center keine Zuweisung vorgenommen und kein Benutzer als Besitzer festgelegt, wird der Benutzer, der sich als erster nach der Installation von SafeGuard Enterprise an den Computer anmeldet, als Besitzer eingetragen. Dieser Benutzer kann weiteren Benutzern die Anmeldung an diesem Computer ermöglichen (siehe Registrieren weiterer SafeGuard Enterprise-Benutzer (Seite 106). Werden im SafeGuard Management Center diesem Computer nachträglich Benutzer zugewiesen, so können sich diese dann auch in der SafeGuard Power-On Authentication anmelden. Voraussetzung dafür ist allerdings, dass es sich um komplette Benutzer (deren Zertifikat und Schlüssel bereits existieren) handelt. Die Erlaubnis durch den Besitzer des Computers ist dann nicht notwendig.

Über folgende Einstellungen kann festgelegt werden, wem es erlaubt ist, weitere Benutzer in die UMA aufzunehmen:

- **Kann Besitzer werden** Die Auswahl dieser Einstellung ist Voraussetzung dafür, dass ein Benutzer als Besitzer eines Computers eingetragen werden kann.

- **Benutzer ist Besitzer**: Ist diese Einstellung ausgewählt, wird dieser Benutzer als Besitzer in die UMA eingetragen. Es kann jeweils nur ein Benutzer pro Computer als Besitzer in der UMA eingetragen werden.

  Wer Benutzer in die UMA aufnehmen darf, wird zusätzlich über die Richtlinieneinstellung **Registrieren von neuen SGN-Benutzern erlauben** in einer Richtlinie vom Typ **Spezifische Computereinstellungen** gesteuert. Die Einstellung **Registrierung von SGN Windows-Benutzern aktivieren** in Richtlinien vom Typ **Spezifische Computereinstellungen** legt fest, ob SGN Windows-Benutzer auf dem Endpoint registriert und zur UMA hinzugefügt werden können.

- **Registrieren von neuen SGN-Benutzern erlauben**

  Niemand

  Auch der als Besitzer eingetragene Benutzer kann keinen weiteren Benutzern die Aufnahme in die UMA ermöglichen. Die Funktionalität, dass ein Besitzer weitere Aufnahmen ermöglichen kann, wird damit deaktiviert.

  Besitzer (Standardeinstellung)

  Hinweis: Ein Sicherheitsbeauftragter kann im SafeGuard Management Center immer Benutzer hinzufügen.

  Jeder

  Hebt die Einschränkung auf, dass nur der Besitzer Benutzer hinzufügen darf.

  Hinweis: Bei Endpoints, auf denen das Device Encryption-Modul nicht installiert ist, muss die Einstellung **Registrieren von neuen SGN-Benutzern erlauben** auf **Jeder** gesetzt sein, wenn es auf dem Endpoint möglich sein soll, der UMA mehrere Benutzer hinzuzufügen, die Zugriff auf ihre Schlüsselringe haben sollen. Sonst können Benutzer nur im Management Center hinzugefügt werden. Diese Option ist wird nur auf zentral verwalteten Endpoints ausgewertet. Siehe auch Neue SafeGuard Enterprise Data Exchange-Benutzer erhalten nach dem Anmelden bei SafeGuard Enterprise Data Exchange Only Clients kein Zertifikat.

- **Registrierung von SGN Windows-Benutzern aktivieren**

  Wenn Sie **Ja** auswählen, können SGN Windows-Benutzer auf dem Endpoint registriert werden. Ein SGN Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er auf verschlüsselte Dateien zugreifen kann

wie ein SGN-Benutzer. Wenn Sie diese Einstellung wählen, werden alle Benutzer, die andernfalls SGN-Gast-Benutzer geworden wären, zu SGN Windows-Benutzern. Die Benutzer werden zur UMA hinzugefügt, sobald sie sich an Windows angemeldet haben. SGN Windows-Benutzer lassen sich auf zentral verwalteten Endpoints automatisch und auf Standalone-Endpoints manuell aus der UMA entfernen. Weitere Informationen finden Sie unter Spezifische Computereinstellungen - Grundeinstellungen (Seite 156).

Beispiel:

Das folgende Beispiel zeigt, wie Sie im SafeGuard Management Center festlegen können, dass sich ausschließlich drei bestimmte Benutzer (Benutzer_a, Benutzer_b, Benutzer_c) auf dem Computer Computer_ABC anmelden können.

Ausgangssituation: Sie legen im SafeGuard Management Center das gewünschte Verhalten fest. SafeGuard Enterprise wird in der Nacht auf allen Endpoints installiert. Am Morgen sollen sich die Benutzer an ihrem Computer anmelden können.

1. Weisen Sie im SafeGuard Management Center Benutzer_a, Benutzer_b, Benutzer_c dem Computer Computer_ABC zu. (**Benutzer & Computer** -> Computer_ABC auswählen -> Benutzer via Drag&Drop zuweisen). Damit haben Sie eine UMA festgelegt.
2. Setzen Sie in einer Richtlinie vom Typ **Spezifische Computereinstellungen** die Einstellung **Registrieren von neuen SGN-Benutzern erlauben** auf **Niemand**. Da es Benutzer_a, Benutzer_b, Benutzer_c nicht erlaubt werden soll, Benutzer hinzuzufügen, ist es nicht notwendig, einen Benutzer als Besitzer festzulegen.
3. Weisen Sie die Richtlinie dem Computer zu bzw. an einer Stelle in der Verzeichnisstruktur zu, wo sie für den Computer wirksam wird.

Bei der Anmeldung des ersten Benutzers an Computer_ABC wird ein Autologon für die SafeGuard POA ausgeführt. Die Computerrichtlinien werden an den Endpoint geschickt. Da Benutzer_a in der UMA eingetragen ist, wird er im Zuge der Windows-Anmeldung komplettiert. Seine Benutzerrichtlinien, Zertifikate und Schlüssel werden an den Endpoint geschickt. Die SafeGuard POA wird aktiviert.

Hinweis: Der Benutzer kann über die Statusausgabe im SafeGuard Tray Icon überprüfen, wann dieser Vorgang abgeschlossen ist.

Benutzer_a existiert nun als kompletter Benutzer in SafeGuard Enterprise und kann sich bei der nächsten Anmeldung in der SafeGuard POA authentisieren und wird automatisch angemeldet.

Benutzer_a fährt nun den Computer herunter und Benutzer_b will sich anmelden. Da die SafeGuard POA aktiviert ist, findet kein Autologon mehr statt.

Für die Benutzer_b und Benutzer_c gibt es nun zwei Möglichkeiten, Zugang zu diesem Computer zu erlangen.

- Benutzer_a deaktiviert im SafeGuard POA-Anmeldedialog die Option **Durchgehende Anmeldung an Windows** und meldet sich an.
- Benutzer_b authentisiert sich über Challenge/Response in der SafeGuard POA.

In beiden Fällen wird anschließend der Windows-Anmeldedialog angezeigt.

Benutzer_b kann dort seine Windows-Anmeldeinformationen eingeben. Seine Benutzerrichtlinien, Zertifikate und Schlüssel werden an den Endpoint geschickt. Er wird in der SafeGuard POA aktiviert. Benutzer_b existiert nun als kompletter Benutzer in SafeGuard Enterprise. Er kann sich bei der nächsten Anmeldung in der SafeGuard POA authentisieren und wird automatisch angemeldet.

Es wurde in der Computerrichtlinie zwar festgelegt, dass auf diesem Computer niemand Benutzer importieren darf, da sie sich aber bereits in der UMA befinden, können Benutzer_b und Benutzer_c durch die Windows-Anmeldung dennoch komplettiert und in der SafeGuard POA aktiviert werden.

Alle anderen Benutzer werden nicht in die UMA aufgenommen und können sich daher niemals an der SafeGuard Power-on Authentication authentisieren. Alle Benutzer, die sich an Windows anmelden und nicht Benutzer_a, Benutzer_b oder Benutzer_c sind, werden in diesem Szenario nicht in die UMA aufgenommen und daher auch nie in der SafeGuard POA aktiv.

Sie können im SafeGuard Management Center später weitere Benutzer hinzufügen. Allerdings steht ihr Schlüsselring nach der ersten Anmeldung noch nicht zur Verfügung, da eine Synchronisierung erst durch diese Anmeldung angestoßen wird. Nach einer erneuten Anmeldung steht auch der Schlüsselring zur Verfügung und die Benutzer können entsprechend den geltenden Richtlinien auf den Computer zugreifen. Haben sie sich zuvor noch an keinem Endpoint erfolgreich angemeldet, können sie wie zuvor beschrieben aufgenommen werden.

Hinweis: Wenn das letzte gültige Benutzerzertifikat von einem SO oder MSO aus der UMA entfernt wurde, kann jeder Benutzer die SafeGuard POA des entsprechenden Computers absolvieren. Dasselbe gilt, wenn sich die Domain des Endpoints ändert. Dann sind nur Windows-Anmeldeinformationen zum Anmelden am Computer, zum Reaktivieren der SafeGuard POA und das Hinzufügen als neuer Besitzer nötig.

26.1.1 Benutzer sperren

Durch Auswählen des Kontrollkästchens in der Spalte **Benutzer sperren** wird dem Benutzer die Anmeldung an diesem Computer verboten. Wenn der betreffende Benutzer angemeldet ist, wenn eine Richtlinie, die diese Einstellung enthält, wird der Benutzer abgemeldet.

26.1.2 Gruppen

Im SafeGuard Management Center können auch Computergruppen einem Benutzer (Konto) bzw. Benutzergruppen einem Computer zugewiesen werden.

So erstellen Sie eine Gruppe: Klicken Sie unter **Benutzer & Computer** mit der rechten Maustaste auf den relevanten Objektknoten, bei dem Sie die Gruppe erstellen möchten. Wählen Sie dann **Neu** und **Neue Gruppe erzeugen**. Geben Sie in **Neue Gruppe erzeugen** unter **Vollst. Name** den Namen der Gruppe und nach Wunsch eine Beschreibung ein. Klicken Sie auf **OK**.

Beispiel: Service-Konto

Auf diese Weise ist es z. B. einfach möglich, über ein Service-Konto eine große Anzahl Computer zu warten. Dazu müssen sich die Computer in einer Gruppe befinden. Diese Gruppe wird dann einem Service-Konto (Benutzer) zugewiesen. Der Besitzer des Service-Kontos kann sich dann an alle Computer dieser Gruppe anmelden.

Ebenso kann durch das Zuweisen einer Gruppe, die verschiedene Benutzer enthält, diesen Benutzern in einem einfachen Schritt die Anmeldung an einem bestimmten Computer ermöglicht werden.

26.2 Zuweisen von Benutzer- und Computergruppen

Um die Benutzer und Computer Zuordnung unter **Benutzer & Computer** einzusehen, benötigen Sie mindestens das Zugriffsrecht **Schreibgeschützt** für eines der beteiligten Objekte (Benutzer oder Computer). Um die Zuweisung zu definieren oder zu ändern, benötigen Sie

das Zugriffsrecht **Voller Zugriff** für beide beteiligten Objekte. Die UMA-Anzeige zeigt die verfügbaren Benutzer/Maschinen gefiltert nach Ihren Zugriffsrechten.

Hinweis: Das Zuweisen einzelner Benutzer an einen Computer oder umgekehrt, funktioniert analog zur Beschreibung für Gruppen.

1. Klicken Sie auf **Benutzer & Computer**.
2. Zum Zuweisen einer Gruppe von Computern zu einem Benutzer markieren Sie den Benutzer.
3. Klicken Sie im Aktionsbereich auf die Registerkarte **Computer**.

   Unter **Verfügbare Computer** werden alle Computer und Computergruppen angezeigt.

4. Ziehen Sie die gewünschten Gruppen aus der Liste der **Verfügbaren Gruppen** in den Aktionsbereich.
5. Ein Dialog, in dem Sie gefragt werden, ob der Benutzer Besitzer aller Computer werden können soll, wird angezeigt.

   Ist für einen Computer im SafeGuard Management Center kein Besitzer festgelegt, wird der erste Benutzer, der sich an diesen Computer anmeldet, automatisch als Besitzer eingetragen. Damit hat er das Recht, anderen Benutzern Zugriff auf diesen Computer zu erlauben. Voraussetzung dafür ist, dass er das Recht **Kann Besitzer werden** besitzt.

   - Beantworten Sie diese Frage mit **Ja**, kann der Benutzer, wenn er sich als erster an diesen Computer anmeldet, Besitzer werden und damit weiteren Benutzern Zugriff gewähren.
   - Beantworten Sie diese Frage mit **Nein**, ist der Benutzer nicht Besitzer dieses Computers.

   Für ein Service-Konto ist es in der Regel nicht notwendig, dass der Inhaber dieses Kontos Besitzer der Computer werden kann. Diese Einstellung kann nach der initialen Zuweisung geändert werden.

Nach der Beantwortung der Frage werden alle Computer aus der zugewiesenen Gruppe im Aktionsbereich angezeigt.

Der Benutzer darf sich jetzt an allen Computern anmelden, die so zugewiesen wurden.

Die Zuweisung einer Benutzergruppe an einen einzelnen Computer funktioniert analog zu dieser Beschreibung.

27 Token und Smartcards

Hinweis: Token und Smartcards können nicht für Mac OS X Endpoints konfiguriert werden.

SafeGuard Enterprise bietet erweiterte Sicherheit durch die Unterstützung von Token und Smartcards für die Authentisierung. Auf Token/Smartcards lassen sich Zertifikate, digitale Signaturen und biometrische Informationen speichern.

Die Token-Authentisierung basiert auf dem Prinzip der Zwei-Faktor-Authentisierung: Ein Benutzer verfügt über einen Token (Besitz), kann den Token aber nur nutzen, wenn er das spezifische Token-Kennwort kennt (Wissen). Bei Verwendung eines Token oder einer Smartcard benötigen die Benutzer zur Authentisierung nur noch den Token und eine PIN.

Hinweis: Smartcards und Token werden aus Sicht von SafeGuard Enterprise gleich behandelt. Deshalb werden im Produkt und in der Hilfe die Begriffe "Token" und "Smartcard" gleichgesetzt. Die Verwendung von Token und Smartcards muss in der Lizenz aktiviert werden (siehe Token-Lizenzen (Seite 28)).

Hinweis: Bei Windows 8 und höher gibt es eine Funktion namens *virtuelle Smartcard*. Eine virtuelle Smartcard simuliert mit Hilfe eines TPM-Chip als Basis die Funktionalität einer physischen Smartcard, kann aber nicht mit SafeGuard Enterprise genutzt werden.

SafeGuard Enterprise unterstützt Token:

- in der SafeGuard Power-on Authentication (gilt nicht für Windows 8 und Windows 8.1)
- auf Betriebssystemebene
- zur Anmeldung am SafeGuard Management Center

Wenn ein Token für einen Benutzer in SafeGuard Enterprise ausgestellt wird, werden Daten wie Hersteller, Typ, Seriennummer, Anmeldedaten und Zertifikate in der SafeGuard Enterprise-Datenbank hinterlegt. Token werden anhand der Seriennummer identifiziert und sind dann in SafeGuard Enterprise bekannt.

Es ergeben sich erhebliche Vorteile:

- Sie wissen, welche Token im Umlauf sind und welchen Benutzern sie zugeordnet sind.
- Sie wissen, wann sie ausgestellt wurden.
- Wenn Token verlorengegangen sind, kann der Sicherheitsbeauftragte sie identifizieren und für die Authentisierung sperren. Damit kann Datenmissbrauch verhindert werden.
- Trotzdem kann der Sicherheitsbeauftragte über Challenge/Response die Anmeldung ohne Token zeitweilig erlauben, z. B. wenn ein Benutzer seine PIN vergessen hat.

  Hinweis: Bei SafeGuard volume-basierender Verschlüsselung wird diese Recovery-Option für die Anmeldung mit kryptographischen Token (Kerberos) nicht unterstützt.

27.1 Token-Typen

Der Begriff "Token" bezieht sich auf alle verwendeten Technologien und ist nicht an eine bestimmte Form von Gerät gebunden. Dies umfasst alle Geräte, die Daten für die Identifizierung

und Authentisierung speichern und übertragen können, zum Beispiel Smartcards und USB-Token.

SafeGuard Enterprise unterstützt die folgenden Token/Smartcard-Typen für die Authentisierung:

- **Nicht kryptographisch**

  Die Authentisierung in der SafeGuard POA und in Windows erfolgt auf der Grundlage der auf dem Token gespeicherten Anmeldedaten (Benutzername/Kennwort).

- **kryptographisch - Kerberos**

  Die Authentisierung in der SafeGuard POA und in Windows erfolgt auf der Grundlage der auf dem Token gespeicherten Zertifikate.

  Hinweis: Kryptographische Token können nicht für Standalone-Endpoints verwendet werden.

27.1.1 Kryptographische Token - Kerberos

Bei der Verwendung von kryptographischen Token erfolgt die Authentisierung in der SafeGuard POA über das Zertifikat auf dem Token. Zur Anmeldung müssen die Benutzer nur die PIN des Token eingeben.

Hinweis: Kryptographische Token können nicht für Standalone-Endpoints verwendet werden.

Den Benutzern müssen vollständig ausgestellte Token bereitgestellt werden. Weitere Informationen finden Sie unter Konfigurieren der Token-Benutzung (Seite 220).

Grundlegende Anforderungen für Zertifikate:

- Algorithmus: RSA
- Schlüssellänge: mindestens 1024.
- Verwendung des Schlüssels: *Datenverschlüsselung* oder *Schlüsselverschlüsselung*. Dies kann per Richtlinie außer Kraft gesetzt werden.
- Selbst-signiert: Nein. Dies kann per Richtlinie außer Kraft gesetzt werden.

Hinweis: Bei Problemen bei der Anmeldung mit einem Kerberos-Token kann weder Challenge/Response noch Local Self Help für Recovery-Vorgänge benutzt werden. Hier wird nur Challenge/Response mit virtuellen Clients unterstützt. Mit diesem Verfahren können Benutzer wieder Zugriff auf verschlüsselte Volumes auf Ihren Endpoints erlangen.

27.2 Komponenten

Für die Benutzung von Token/Smartcards in Verbindung mit SafeGuard Enterprise sind folgende Komponenten erforderlich:

- Token/Smartcard
- Token-/Smartcard-Lesegerät
- Token-/Smartcard-Treiber
- Token/Smartcard Middleware (PKCS#11-Modul)

USB-Token

USB-Token bestehen aus einer Smartcard und einem Smartcard-Leser, wobei sich die beiden Einheiten in einem Gehäuse befinden. Für die Benutzung von USB Token ist ein USB Port erforderlich.

27.2.1 Token/Smartcards-Lesegeräte und Treiber

- **Windows**

  Auf Windows-Betriebssystemebene werden PC/SC-kompatible Kartenleser unterstützt. Die PC/SC-Schnittstelle regelt die Kommunikation zwischen Computer und Smartcard. Viele dieser Kartenleser sind bereits Teil der Windows-Installation. Smartcards benötigen PKCS#11 kompatible Smartcard-Treiber, damit sie von SafeGuard Enterprise unterstützt werden können.

- **Power-on Authentication aktivieren**

  An der SafeGuard Power-on Authentication wird die PC/SC-Schnittstelle unterstützt, die die Kommunikation zwischen Computer und Smartcard regelt. Die unterstützten Smartcard-Treiber sind fest implementiert und die Benutzer können keine zusätzlichen Treiber hinzufügen. Die passenden Smartcard-Treiber müssen über eine Richtlinie in SafeGuard Enterprise aktiviert werden.

  Die Schnittstelle für Smartcard-Leser ist standardisiert und viele Kartenleser haben eine USB-Schnittstelle oder eine ExpressCard/54-Schnittstelle und implementieren den CCID-Standard. In SafeGuard Enterprise ist dies eine Voraussetzung für die Unterstützung in der SafeGuard Power-on Authentication. Außerdem muss auf Treiber-Seite das PKCS#11-Modul unterstützt werden.

27.2.2 Unterstützte Token/Smartcards an der SafeGuard Power-on Authentication

SafeGuard Enterprise unterstützt eine breite Palette an Smartcards/Smartcard-Lesegeräten, USB-Token mit den entsprechenden Treibern und Middleware in der SafeGuard Power-on Authentication. In SafeGuard Enterprise werden Token/Smartcards unterstützt, die 2.048 Bit RSA-Operationen unterstützen.

Da die Unterstützung von Token/Smartcards von Release zu Release erweitert wird, werden die in der jeweils aktuellen SafeGuard Enterprise Version unterstützten Token und Smartcards in den Release Notes aufgeführt.

27.2.3 Unterstützte Middleware

Die in der folgenden Liste aufgeführte Middleware wird über deren jeweiliges PKCS#11-Modul unterstützt. PKCS#11 ist eine standardisierte Schnittstelle zur Anbindung kryptographischer Token/Smartcards an verschiedenste Software. Hier dient PKCS#11 der Kommunikation zwischen kryptographischen Token/Smartcard, Smartcard-Leser und SafeGuard Enterprise. Siehe auch http://www.sophos.com/de-de/support/knowledgebase/112781.aspx.

Hersteller	Middleware
ActivIdentity	ActivClient, ActivClient (PIV)
AET	SafeSign Identity Client
Aladdin	eToken PKI Client

Hersteller	Middleware
A-Trust	a.sign Client
Charismatics	Smart Security Interface
Gemalto	Gemalto Access Client, Gemalto Classic Client, Gemalto .NET Card
IT Solution GmbH	IT Solution trustWare CSP+
Nexus	Nexus Personal
RSA	RSA Authentication Client 2.x, RSA Smart Card Middleware 3.x
Sertifitseerimiskeskus AS	Estonian ID Card
Siemens	CardOS API TC-FNMT
ATOS	CardOS API TC-FNMT
FNMT	Módulo PCKS#11 TC-FNMT TC-FNMT
T-Systems	NetKey 3.0
Unizeto	proCertum

Lizenzen

Beachten Sie, dass für die Benutzung der jeweiligen Middleware für das Standard-Betriebssystem eine Lizenzvereinbarung mit dem jeweiligen Hersteller erforderlich ist. Informationen zum Erhalt der Lizenzen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/116585.aspx.

Wenn Sie Siemens-Lizenzen erwerben möchten, wenden Sie sich an:

Atos IT Solutions and Services GmbH

Otto-Hahn-Ring 6

81739 München

Germany

Die Middleware wird in einer SafeGuard Enterprise-Richtlinie vom Typ **Spezifische Computereinstellungen** unter **Benutzerdefinierte PKCS#11 Einstellungen** im Feld **PKCS#11 Modul für Windows** oder **PKCS#11 Modul für die Power-on Authentication** angegeben. Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem Computer installiert sein, auf dem das SafeGuard Management Center läuft.

27.3 Konfigurieren der Token-Benutzung

Führen Sie die folgenden Handlungsschritte aus, wenn Sie den folgenden Benutzern Token für die Authentisierung bereitstellen möchten:

- Benutzer von zentral verwalteten Endpoints
- Sicherheitsbeauftragte des SafeGuard Management Center

1. Initialisierung leerer Token

   Weitere Informationen finden Sie unter Initialisierung von Token (Seite 221).

2. Installation der Middleware

   Weitere Informationen finden Sie unter Installation von Middleware (Seite 221).

3. Aktivierung der Middleware

   Weitere Informationen finden Sie unter Aktivierung von Middleware (Seite 221).

4. Ausstellen von Token für Benutzer und Sicherheitsbeauftragte

   Weitere Informationen finden Sie unter Ausstellen eines Token (Seite 221).

5. Konfigurieren des Anmeldemodus

   Weitere Informationen finden Sie unter Konfiguration des Anmeldemodus (Seite 223).

6. Konfigurieren weiterer Token-Einstellungen, zum Beispiel Syntaxregeln für PINs.

   Weitere Informationen finden Sie unter Verwalten von PINs (Seite 228) und Verwalten von Token und Smartcards (Seite 229).

7. Zuweisen von Zertifikaten und Schlüsseln zu Token/Benutzern

   Weitere Informationen finden Sie unter Zuweisung von Zertifikaten (Seite 225).

Sie können auch einen bereits mit Daten einer anderen Anwendung versehenen Token zur Authentisierung verwenden, sofern genügend freier Speicherplatz für die Zertifikate und Anmeldeinformationen darauf vorhanden ist.

Für die einfache Token-Verwaltung bietet SafeGuard Enterprise folgende Funktionen:

- Token-Informationen anzeigen und filtern
- PINs initialisieren, ändern, zurücksetzen und sperren
- Token-Daten lesen und löschen
- Token sperren

Hinweis: Um Token auszustellen und zu verwalten oder Daten auf ausgestellten Token zu ändern, benötigen Sie das Zugriffsrecht **Voller Zugriff** für die relevanten Benutzer. Die Ansicht **Ausgestellte Token** zeigt die Token für alle Benutzer, für die Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** haben.

27.4 Vorbereitung für die Benutzung von Token

Die folgenden vorbereitenden Maßnahmen sind für die Unterstützung von Token/Smartcards in SafeGuard Enterprise notwendig:

- Initialisierung leerer Token
- Installation der Middleware

- Aktivierung der Middleware

27.4.1 Initialisieren eines Token

Bevor ein "leerer", unformatierter Token in SafeGuard Enterprise bentutzt werden kann, muss er nach den Angaben des Token-Herstellers für die Verwendung vorbereitet, also initialisiert werden. Bei der Initialisierung wird er mit Basisinformationen, z. B. den Standard-PINs, beschrieben. Dies erfolgt mit der Initialisierungssoftware des Herstellers.

Weitere Informationen finden Sie in der Dokumentation des relevanten Token-Herstellers.

27.4.2 Installation von Middleware

Installieren Sie die korrekte Middleware sowohl auf dem Computer, auf dem das SafeGuard Management Center installiert ist, als auch auf dem relevanten Endpoint, falls noch nicht geschehen. Informationen über unterstützte Middleware finden Sie unter Unterstützte Middleware (Seite 218).

Starten Sie die Computer, auf denen Sie die neue Middleware installiert haben, neu.

Hinweis: Wenn Sie **Gemalto .NET Card** oder **Nexus Personal** Middleware installieren, müssen Sie den Installationspfad der Middleware auch zur PATH-Umgebungsvariable der **Systemeigenschaften** Ihres Computers hinzufügen.

- Standard-Installationspfad für **Gemalto .NET Card**: `C:\Programme\Gemalto\PKCS11 for .NET V2 smart cards`
- Standard-Installationspfad für **Nexus Personal**: `C:\Programme\Personal\bin`

27.4.3 Aktivieren der Middleware

Sie müssen im SafeGuard Management Center über eine Richtlinie die passende Middleware in Form des PKCS#11-Moduls zuweisen. Dies müssen Sie sowohl für den Computer, auf dem das SafeGuard Management Center läuft, als auch für den Endpoint erledigen. Dann erst kann SafeGuard Enterprise mit dem Token kommunizieren. Die Einstellung für das PKCS#11-Modul können Sie folgendermaßen über eine Richtlinie festlegen.

Voraussetzung: Die Middleware wurde auf dem entsprechenden Computer installiert und der Token wurde initialisiert. Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem Computer installiert sein, auf dem das SafeGuard Management Center läuft.

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Legen Sie eine neue Richtlinie des Typs **Spezifische Computereinstellungen** an oder wählen Sie eine bereits bestehende Richtlinie dieses Typs aus.
3. Wählen Sie im rechten Arbeitsbereich unter **Tokenunterstützung > Modulname** die passende Middleware aus. Speichern Sie die Einstellungen.
4. Weisen Sie die Richtlinie zu.

SafeGuard Enterprise kann nun mit dem Token kommunizieren.

27.5 Ausstellen eines Token

Beim Ausstellen eines Token in SafeGuard Enterprise werden Daten auf den Token geschrieben, die dann für die Authentisierung verwendet werden. Bei den Daten handelt es sich um die Anmeldeinformationen und Zertifikate.

In SafeGuard Enterprise können Token für folgende Benutzerrollen ausgestellt werden:

- Token für Endbenutzer von zentral verwalteten Endpoints.
- Token für Sicherheitsbeauftragte (SO)

Zugriff auf den Token haben sowohl der Benutzer als auch der Sicherheitsbeauftragte (SO). Der Benutzer ist der, der den Token benutzen soll. Nur er hat Zugriff auf private Objekte und Schlüssel. Der SO hat nur Zugriff auf öffentliche Objekte, kann allerdings die Benutzer-PIN zurücksetzen.

27.5.1 Ausstellen eines Token oder einer Smartcard für Benutzer

Voraussetzungen:

- Der Token muss initialisiert und das passende PKCS#11-Modul aktiviert worden sein.
- Das SafeGuard Enterprise Client-Konfigurationspaket muss zudem auf dem Computer installiert sein, auf dem das SafeGuard Management Center läuft.
- Sie benötigen das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
3. Wählen Sie den Benutzer, für den ein Token ausgestellt werden soll, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Token-Daten**.
4. Gehen Sie in der Registerkarte **Token-Daten** wie folgt vor:
   a) Wählen Sie die **Benutzer-ID** und **Domäne** des betreffenden Benutzers aus und geben Sie sein Windows-**Kennwort** ein.
   b) Klicken Sie auf **Token ausstellen**.

   Der Dialog **Token ausstellen** wird angezeigt.
5. Wählen Sie den relevanten Slot aus der **Verfügbare Slots** Dropdownliste aus.
6. Vergeben Sie eine neue **Benutzer-PIN** und wiederholen Sie die Eingabe.
7. Geben Sie unter **SO-PIN** die vom Hersteller erhaltene Standard-PUK bzw. die bei der Token-Initialisierung vergebene PIN ein.

   Hinweis: Wenn Sie nur das Feld **Benutzer-PIN (erforderlich)** ausfüllen, muss die Benutzer-PIN mit der PIN übereinstimmen, die bei der Token-Initialisierung vergeben wurde. Sie müssen die Benutzer-PIN dann nicht wiederholen und keine SO-PIN eingeben.
8. Klicken Sie auf **Token jetzt ausstellen**.

Der Token wird ausgestellt, die Anmeldeinformationen auf den Token geschrieben und die Token-Informationen in der SafeGuard Enterprise-Datenbank hinterlegt. Im Bereich **Token** können Sie sich in der Registerkarte **Token-Information** die Daten anzeigen lassen.

27.5.2 Ausstellen eines Token oder einer Smartcard für einen Sicherheitsbeauftragten

Bei der Erstinstallation von SafeGuard Enterprise besteht für den ersten Sicherheitsbeauftragten bereits die Möglichkeit, sich einen Token ausstellen zu lassen und den Anmeldemodus festzulegen (siehe *SafeGuard Enterprise Installationsanleitung*). Für alle

weiteren Sicherheitsbeauftragten nehmen Sie die Ausstellung eines Token im SafeGuard Management Center vor.

Voraussetzung:

- Der Token muss initialisiert und das passende PKCS#11-Modul aktiviert worden sein.
- Sie benötigen die Rechte, die Angaben für den Sicherheitsbeauftragten festlegen zu dürfen.

1. Klicken Sie im SafeGuard Management Center auf **Sicherheitsbeauftragte**.
2. Stecken Sie den Token an der USB-Schnittstelle ein. SafeGuard Enterprise liest den Token ein.
3. Markieren Sie im linken Navigationsfenster **Sicherheitsbeauftragte** und wählen Sie im Kontextmenü **Neu > Neuer Sicherheitsbeauftragter**.

   Der Dialog **Neuen Sicherheitsbeauftragten erstellen** wird angezeigt.

4. Geben Sie im Feld **Token-Anmeldung** die Art der Anmeldung für den Sicherheitsbeauftragten ein:
   - Wenn sich der Sicherheitsbeauftragte wahlweise mit oder ohne Token authentisieren soll, wählen Sie **Optional**.
   - Um festzulegen, dass sich der Sicherheitsbeauftragte mit Token anmelden muss, wählen Sie **Zwingend erforderlich**.

     Bei dieser Einstellung verbleibt der private Schlüssel auf dem Token. Der Token muss immer eingesteckt sein, ansonsten wird ein Neustart des Systems notwendig.

5. Geben Sie als nächstes das Zertifikat des Sicherheitsbeauftragten an.
   - Um ein neues Zertifikat zu erzeugen, klicken Sie auf die Schaltfläche **Erzeugen** neben der **Zertifikat** Dropdown-Liste.

     Geben Sie das Kennwort für das Zertifikat zweimal ein und klicken Sie auf **OK**.

     Legen Sie den Speicherort für das Zertifikat fest.
   - Um Zertifikate zu importieren, klicken Sie auf die Schaltfläche **Importieren** neben der **Zertifikat** Dropdown-Liste, um die entsprechende Zertifikatsdatei zu öffnen.

     Nach Zertifikaten wird zuerst in einer Zertifikatsdatei, dann auf dem Token gesucht. Die Zertifikate können an den jeweiligen Speicherorten verbleiben.

6. Aktivieren Sie die Rollen und Domänen, die dem Beauftragten zugewiesen werden sollen, unter **Rollen**.
7. Bestätigen Sie die Eingaben mit **OK**.

Der Sicherheitsbeauftragte wird angelegt, der Token wird ausgestellt, die Anmeldedaten werden je nach Einstellung auf den Token geschrieben und die Token-Informationen werden in der SafeGuard Enterprise-Datenbank hinterlegt. Im Bereich **Token** können Sie sich in der Registerkarte **Token-Information** die Daten anzeigen lassen.

27.6 Konfigurieren des Anmeldemodus

Für die Anmeldung von Endbenutzern mit einem Token gibt es zwei Anmeldeformen. Eine Kombination der beiden Anmeldeformen ist möglich.

- Anmeldung mit Benutzername/Kennwort
- Anmeldung mit Token

Wenn Sie sich mit einem Token oder einer Smartcard anmelden, können Sie zwischen einem Token-Anmeldemodus mit nicht-kryptographischem Token oder mit Kerberos-Unterstützung (kryptographisch) wählen.

Als Sicherheitsbeauftragter legen Sie den zu verwendenden Anmeldemodus in einer Sicherheitsrichtlinie vom Typ **Authentisierung** fest.

Auswahl der Token-Anmeldeoption **Kerberos**:

- Sie müssen ein Zertifikat in einer PKI ausstellen und es auf dem Token ablegen. Dieses Zertifikat wird als Benutzerzertifikat in die SafeGuard Enterprise Datenbank importiert. Falls dort bereits ein automatisch erzeugtes Zertifikat existiert, wird es durch das importierte Zertifikat überschrieben.

27.6.1 Aktivieren der automatischen Anmeldung an der SafeGuard POA mit Default-Token-PIN

Eine per Richtlinie verteilte Default-Token-PIN ermöglicht die automatische Benutzeranmeldung an der SafeGuard Power-on Authentication. Somit muss nicht jeder einzelne Token separat ausgestellt werden und die Benutzer können sich ohne Benutzerinteraktion automatisch an der SafeGuard Power-on Authentication anmelden.

Wenn bei der Anmeldung ein Token benutzt wird und dem Computer eine Default-PIN zugeordnet ist, wird eine durchgehende Anmeldung an der SafeGuard Power-on Authentication durchgeführt. Der Benutzer muss hier keine PIN eingeben.

Als Sicherheitsbeauftragter können Sie diese spezifische PIN in einer Richtlinie vom Typ **Authentisierung** festlegen und sie verschiedenen Computern oder Computergruppen, z. B. allen Computern eines Standorts, zuordnen.

So aktivieren Sie die automatische Anmeldung mit einer Default-Token-PIN:

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Wählen Sie eine Richtlinie vom Typ **Authentisierung** aus.
3. Wählen Sie unter **Anmeldeoptionen** bei **Anmeldemodus** die Option **Token**.
4. Geben Sie bei **PIN für automatische Anmeldung mit Token** die Default-PIN an, die für die automatische Anmeldung verwendet werden soll. In diesem Fall müssen keine PIN-Regeln beachtet werden.

   Hinweis: Diese Einstellung steht nur dann zur Verfügung, wenn Sie als möglichen **Anmeldemodus** die Option **Token** gewählt haben.

5. Wählen Sie bei **Durchgehende Anmeldung an Windows** die Option **Durchgehende Anmeldung deaktivieren**. Wenn Sie diese Einstellung nicht auswählen und eine Default-PIN angeben, können Sie die Richtlinie nicht speichern.

   Wenn Sie die **Durchgehende Anmeldung an Windows** dennoch aktivieren möchten, können Sie eine weitere Richtlinie vom Typ **Authentisierung** mit der aktivierten Option erstellen und sie derselben Computergruppe zuordnen. Im RSOP (Resulting Set of Policies) sind somit beide Richtlinien aktiv.

6. Definieren Sie nach Wunsch weitere Token-Einstellungen.
7. Speichern Sie Ihre Einstellungen und ordnen Sie die Richtlinie den relevanten Computern oder Computergruppen zu.

Wenn die automatische Anmeldung auf dem Endpoint erfolgreich durchgeführt werden konnte, wird Windows gestartet.

Schlägt die automatische Anmeldung auf dem Endpoint fehl, so wird der Benutzer an der SafeGuard Power-on Authentication aufgefordert, die Token-PIN einzugeben.

27.7 Zuweisung von Zertifikaten

Außer den Anmeldeinformationen können auf einen Token auch Zertifikate geschrieben werden. Es ist möglich, den privaten Teil des Zertifikats (.p12-Datei) ausschließlich auf dem Token zu speichern. Benutzer können sich dann jedoch nur mit dem Token anmelden. Wir empfehlen den Einsatz von PKI-Zertifikaten.

So können Sie Authentisierungsdaten Token zuweisen:

- durch Generieren von Zertifikaten direkt auf dem Token
- durch Zuweisen von Daten, die sich bereits auf dem Token befinden
- durch Importieren von Zertifikaten aus einer Datei

Hinweis: CA-Zertifikate können nicht von einem Token entnommen und in der Datenbank oder im Zertifikatsspeicher gespeichert werden. Wenn Sie CA-Zertifikate verwenden, müssen diese in Dateiform zur Verfügung stehen, nicht nur auf einem Token. Dies gilt auch für CRLs (Certificate Revocation List). Außerdem muss die Kombination von CA-Zertifikaten und CRL zusammenpassen, da ansonsten eine Anmeldung an allen betroffenen Computern nicht mehr möglich ist. Überprüfen Sie, ob CA und die entsprechende CRL korrekt sind. SafeGuard Enterprise übernimmt diese Überprüfung nicht! SafeGuard Enterprise kann dann nur mit ablaufenden Zertifikaten umgehen, wenn der alte und neue private Schlüssel auf demselben Token stehen.

27.7.1 Erzeugen von Zertifikaten durch Token

Um Zertifikate durch Token zu erzeugen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

Sie können neue Zertifikate direkt durch den Token generieren lassen, wenn zum Beispiel keine Zertifikatsinfrastruktur vorhanden ist.

Hinweis: Wird der private Teil des Zertifikats allein auf den Token geschrieben, hat der Benutzer nur mit dem Token Zugriff auf seinen privaten Schlüssel. Der private Schlüssel befindet sich dann nur noch auf dem Token. Wenn der Token verloren geht, ist der Zugriff auf den privaten Schlüssel nicht mehr möglich.

Voraussetzung: Der Token ist ausgestellt.

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Stecken Sie den Token an der USB-Schnittstelle ein.

   SafeGuard Enterprise liest den Token ein.
3. Markieren Sie den Benutzer, für den Sie ein Zertifikat generieren wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Zertifikat**.
4. Klicken Sie auf das Symbol **Neues Zertifikat generieren und Token zuweisen** in der SafeGuard Management Center Symbolleiste. Beachten Sie, dass die Schlüssellänge auf die Tokengröße abgestimmt sein muss.
5. Wählen Sie den Slot aus und geben Sie die Token-PIN ein.
6. Klicken Sie auf **Erzeugen**.

Das Zertifikat wird durch den Token generiert und dem Benutzer zugewiesen.

27.7.2 Zuweisen von Token-Zertifikaten zu einem Benutzer

Voraussetzungen:

- Der Token ist ausgestellt.
- Sie haben das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

So weisen Sie ein auf einem Token verfügbares Zertifikat einem Benutzer zu:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.
2. Stecken Sie den Token an der USB-Schnittstelle ein.

   SafeGuard Enterprise liest den Token ein.

3. Wählen Sie den Benutzer aus, dem Sie ein Zertifikat zuweisen wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Zertifikat**.
4. Klicken Sie auf das Symbol **Zertifikat von Token zuweisen** in der SafeGuard Management Center Symbolleiste.
5. Wählen Sie das passende Zertifikat aus der Liste aus und geben Sie die Token-PIN ein.
6. Klicken Sie auf **OK**.

Das Zertifikat wird dem Benutzer zugewiesen. Einem Benutzer kann jeweils nur ein Zertifikat zugewiesen sein.

27.7.3 Ändern des Zertifikats eines Benutzers

Sie können die für die Anmeldung erforderlichen Zertifikate ändern oder erneuern, indem Sie im SafeGuard Management Center ein neues Zertifikat zuweisen. Das Zertifikat wird als Standby-Zertifikat neben dem bereits vorhandenen Zertifikat zugewiesen. Der Benutzer ändert das Zertifikat auf dem Endpoint, indem er sich mit dem neuen Zertifikat anmeldet.

Hinweis: Sollten Benutzer ihre Token verlieren oder sollten Token manipuliert worden sein, so tauschen Sie die Token nicht aus, indem Sie neue Zertifikate wie hier beschrieben zuweisen. Andernfalls können Probleme auftreten. So ist das alte Token-Zertifikat unter Umständen noch für die Windows-Anmeldung gültig. Solange das alte Zertifikat noch gültig ist, ist die Anmeldung an Windows noch möglich und der Computer kann entsperrt werden. Um eine Anmeldung zu verhindern, sperren Sie den Token.

Standby-Zertifikate können in folgenden Fällen verwendet werden:

- Ändern von durch (kryptographische) Token erzeugten Zertifikaten
- Wechsel von automatisch erzeugten zu durch Token erzeugten Zertifikaten
- Wechsel von Authentisierung per Benutzername/Kennwort zur Authentisierung durch kryptographischen Token (Kerberos).

Voraussetzungen:

- Der neue Token ist ausgestellt.
- Dem Benutzer ist nur ein Zertifikat zugewiesen.
- Sie haben das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

So ändern Sie das Zertifikat für die Token-Anmeldung für einen Benutzer:

1. Klicken Sie im SafeGuard Management Center auf **Benutzer & Computer**.

2. Stecken Sie den Token an der USB-Schnittstelle ein.

   SafeGuard Enterprise liest den Token ein.

3. Wählen Sie den Benutzer aus, für den Sie das Zertifikat ändern wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Zertifikat**.
4. Klicken Sie in der Symbolleiste auf das Symbol für die Aktion, die Sie durchführen möchten.
5. Wählen Sie das relevante Zertifikat aus und geben Sie die Token-PIN ein.
6. Klicken Sie auf **OK**.
7. Übergeben Sie dem Benutzer den neuen Token.

Das Zertifikat wird dem Benutzer als Standby-Zertifikat zugewiesen. Dies wird durch eine Häkchen in der Spalte **Standby** in der **Zertifikate** Registerkarte des Benutzers angegeben.

Nach der Synchronisierung zwischen dem Endpoint und dem SafeGuard Enterprise Server gibt der Status-Dialog auf dem Endpoint an, dass dieser **Bereit für Zertifikatwechsel** ist.

Der Benutzer muss nun einen Zertifikatwechsel auf dem Endpoint-Computer initiieren. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Benutzerhilfe*.

Nach dem Zertifikatwechsel auf dem Endpoint wird das Zertifikat während der nächsten Synchronisierung auch auf dem SafeGuard Enterprise Server erneuert. Dadurch wird das alte Zertifikat aus der **Zertifikate** Registerkarte des Benutzers im SafeGuard Management Center entfernt. Der neue Token ist nun der Standard-Token für den Benutzer.

Hinweis: Im SafeGuard Management Center können beide Zertifikate separat gelöscht werden. Ist nur ein Standby-Zertifikat verfügbar, so wird das nächste Zertifikat als Standardzertifikat zugewiesen.

27.7.4 Importieren eines Zertifikats aus einer Datei auf einen Token

Voraussetzung: Der Token ist ausgestellt.

Für einen Token mit Kerberos-Unterstützung für zentral verwaltete Endpoints müssen Sie diesen Vorgang auswählen. Das Zertifikat muss von SafeGuard Enterprise erkannt werden und auf den Token aufgebracht werden. Falls bereits ein automatisch generiertes Zertifikat existiert, wird es durch das importierte Zertifikat überschrieben.

So fügen Sie den privaten Teil des Zertifikats (.p12-Datei) aus einer Datei auf dem Token hinzu:

1. Klicken Sie im SafeGuard Management Center auf **Token**.
2. Stecken Sie den Token an der USB-Schnittstelle ein.

   SafeGuard Enterprise liest den Token ein.

3. Markieren Sie den Token, auf den Sie den privaten Teil des Zertifikats aufbringen wollen, und öffnen Sie im rechten Arbeitsbereich die Registerkarte **Anmeldeinformationen & Zertifikate**.
4. Klicken Sie auf das Symbol **P12 auf Token** in der SafeGuard Management Center Symbolleiste.
5. Wählen Sie die passende Zertifikatsdatei aus.
6. Geben Sie die Token-PIN und das Kennwort für die .p12-Datei ein und bestätigen Sie mit **OK**.

Der private Teil des Zertifikats wird auf den Token aufgebracht. Sie müssen diesen nun einem Benutzer zuweisen (siehe Zuweisen von Token-Zertifikaten zu einem Benutzer (Seite 226)). Benutzer können sich dann nur mit diesem Token anmelden.

27.8 Verwalten von PINs

Als Sicherheitsbeauftragter können Sie sowohl die Benutzer-PIN als auch die SO-PIN ändern bzw. die Änderung der Benutzer-PIN erzwingen. Dies wird üblicherweise bei der Erstausstellung eines Token notwendig. Außerdem können Sie PINs initialisieren, d. h. neu vergeben und sperren.

Hinweis: Um PINs zu initialisieren, zu ändern oder zu sperren, benötigen Sie das Zugriffsrecht **Voller Zugriff** für alle relevanten Benutzer.

Für Endpoints können Sie weitere PIN-Optionen über Richtlinien festlegen.

Hinweis: Beachten Sie bei PIN-Änderungen, dass manche Token-Hersteller selbst PIN-Regeln festlegen, die den PIN-Regeln von SafeGuard Enterprise widersprechen können. Möglicherweise können PINs deshalb nicht wie gewünscht geändert werden, auch wenn sie den PIN-Regeln von SafeGuard Enterprise entsprechen. Berücksichtigen Sie daher auf jeden Fall die PIN-Regeln des Token-Herstellers. Diese werden im SafeGuard Management Center im Bereich **Token** unter **Token-Information** angezeigt.

Die Verwaltung der PINs wird im SafeGuard Management Center unter **Token** durchgeführt. Der Token ist eingesteckt und links im Navigationsfenster markiert.

27.8.1 Initialisieren einer Benutzer-PIN

Voraussetzungen:

- Die SO-PIN muss bekannt sein.
- Sie benötigen das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Benutzer-PIN initialisieren** Symbol.
2. Geben Sie die SO-PIN ein.
3. Geben Sie die neue Benutzer-PIN ein, wiederholen Sie die Eingabe und bestätigen Sie mit **OK**.

Die Benutzer-PIN wurde initialisiert.

27.8.2 Ändern der SO-PIN

Voraussetzung: Die bisherige SO-PIN (PIN des Sicherheitsbeauftragten) muss bekannt sein.

1. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **PIN des Sicherheitsbeauftragten ändern** Symbol.
2. Geben Sie die alte SO-PIN ein.
3. Geben Sie die neue SO-PIN ein, wiederholen Sie die Eingabe und bestätigen Sie mit **OK**.

Die SO-PIN wurde geändert

27.8.3 Ändern einer Benutzer-PIN

Voraussetzung:

- Die Benutzer-PIN muss bekannt sein.

- Sie benötigen das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Benutzer-PIN ändern** Symbol.
2. Geben Sie die alte und die neue Benutzer-PIN ein, wiederholen Sie die neue Benutzer-PIN und klicken Sie auf **OK**.

Die Benutzer-PIN wurde geändert. Falls Sie die PIN für einen anderen Benutzer geändert haben, teilen Sie ihm die Änderung mit.

27.8.4 Erzwingen einer PIN-Änderung

Um eine PIN-Änderung zu erzwingen, benötigen Sie das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **PIN-Änderung erzwingen** Symbol.

Wenn sich der Benutzer beim nächsten Mal mit dem Token anmeldet, muss er seine Benutzer-PIN ändern.

27.8.5 PIN-Historie

Die PIN-Historie kann gelöscht werden. Klicken Sie dazu auf das Symbol **PIN-Historie löschen**.

27.9 Verwalten von Token und Smartcards

Im Bereich **Token** des SafeGuard Management Centers hat der Sicherheitsbeauftragte folgende Möglichkeiten:

- Einsehen einer Übersicht über die ausgestellten Token und Zertifikate
- Filtern von Übersichten
- Sperren von Token für die Anmeldung
- Lesen oder Löschen der Daten auf einem Token

27.9.1 Anzeigen von Token/Smartcard-Informationen

Als Sicherheitsbeauftragter können Sie sich Informationen über alle oder einzelne ausgestellte Token anzeigen lassen. Sie können auch Übersichten filtern.

Voraussetzung: Der Token muss eingesteckt sein.

1. Klicken Sie im SafeGuard Management Center auf **Token**.

2. Um Informationen zu einzelnen Token anzeigen zu lassen, wählen Sie den gewünschten Token unter **Token Slots**.

   Unter **Token-Information** werden Hersteller, Typ, Seriennummer, Angaben zu Hardware und PIN-Regeln angezeigt. Außerdem sehen Sie, welchem Benutzer der Token zugeordnet ist.

   Hinweis: Unter **Token Slots** werden die ausgestellten Token ungeachtet Ihrer Zugriffsrechte für die relevanten Benutzer angezeigt, damit Sie sehen können, ob der Token in Gebrauch ist oder nicht. Wenn Sie keine Zugriffsrechte oder das Zugriffsrecht **Schreibgeschützt** für den relevanten Benutzer haben, werden alle Token-Daten in den Registerkarten **Token-Information** und **Anmeldeinformationen und Zertifikate** ausgegraut und Sie können den Token nicht verwalten.

3. Um eine Übersicht über Token anzeigen zu lassen, wählen Sie **Ausgestellte Token**. Sie können alle ausgestellten Token anzeigen lassen oder die Übersicht nach Benutzern filtern.

   Es werden die Seriennummer der Token, die Benutzerzuordnung und das Ausstellungsdatum angezeigt. Außerdem erkennen Sie, ob der Token gesperrt ist.

   Hinweis: Die Ansicht **Ausgestellte Token** zeigt die Token für alle Benutzer, für die Sie die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** haben.

27.9.2 Sperren von Token oder Smartcards

Als Sicherheitsbeauftragter können Sie Token sperren. Dies ist z. B. sinnvoll, wenn ein Token verloren gegangen ist.

Um einen Token zu sperren, benötigen Sie das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie im SafeGuard Management Center auf **Token**.
2. Markieren Sie links im Navigationsbereich **Ausgestellte Token**.
3. Wählen Sie den Token, der gesperrt werden soll, und klicken Sie auf das Symbol **Token sperren** in der SafeGuard Management Center Symbolleiste.

Der Token wird für die Authentisierung gesperrt, der zugeordnete Benutzer kann sich nicht mehr damit anmelden. Der Token kann nur mithilfe der SO-PIN entsperrt werden.

27.9.3 Löschen von Token/Smartcard-Daten

Als Sicherheitsbeauftragter können Sie die Daten, die über SafeGuard Enterprise auf den Token geschrieben wurden, vom Token entfernen.

Voraussetzung:

- Der Token muss eingesteckt sein.
- Sie benötigen das Zugriffsrecht **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie im SafeGuard Management Center auf **Token**.
2. Markieren Sie links im Navigationsbereich den relevanten Token unter **Token Slots**.
3. Klicken Sie in der SafeGuard Management Center Symbolleiste auf das **Token löschen** Symbol.
4. Geben Sie die dem Token zugeordnete SO-PIN ein und bestätigen Sie mit **OK**.

Es werden alle Daten entfernt, die von SafeGuard Enterprise verwaltet werden. Zertifikate verbleiben auf dem Token.

Die Benutzer-PIN wird auf 1234 zurückgesetzt.

Auf diese Weise gelöschte Token werden automatisch aus der Liste der ausgestellten Token entfernt.

27.9.4 Lesen von Token/Smartcard-Daten

All Sicherheitsbeauftragter können Sie die Daten auf dem Token mit der Benutzer-PIN lesen.

Voraussetzung:

- Der Token muss eingesteckt sein. Die PIN muss dem Sicherheitsbeauftragten bekannt sein. Oder sie muss initialisiert sein (siehe Initialisieren einer Benutzer-PIN (Seite 228)).
- Sie benötigen die Zugriffsrechte **Schreibgeschützt** oder **Voller Zugriff** für den relevanten Benutzer.

1. Klicken Sie im SafeGuard Management Center auf **Token**.
2. Wählen Sie links im Navigationsbereich unter **Token Slots** den gewünschten Token und wählen Sie die Registerkarte **Anmeldeinformationen und Zertifikate** aus.
3. Klicken Sie auf das Symbol **Anmeldeinformationen des Benutzers abrufen** und geben Sie die Benutzer-PIN für den Token ein.

Die Daten, die sich auf dem Token befinden, werden angezeigt.

28 Sicheres Wake on LAN (WOL)

Im SafeGuard Management Center können Sie Richtlinieneinstellungen für **Sicheres Wake on LAN (WOL)** definieren, um Endpoints für Software-Rollout-Vorgänge vorzubereiten. Nach dem Wirksamwerden einer solchen Richtlinie auf Endpoints werden die notwendigen Parameter (z. B. SafeGuard POA-Deaktivierung und ein Zeitabstand für Wake on LAN) direkt an die Endpoints übertragen, wo sie analysiert werden.

Das Rollout-Team kann durch die zur Verfügung gestellten Kommandos ein Scheduling-Skript so gestalten, dass die größtmögliche Sicherheit des Endpoint trotz deaktivierter SafeGuard POA gewährleistet bleibt.

Hinweis: Wir weisen an dieser Stelle ausdrücklich darauf hin, dass auch das zeitlich begrenzte "Ausschalten" der SafeGuard POA für eine bestimmte Anzahl von Boot-Vorgängen ein Absenken des Sicherheitsniveaus bedeutet.

Die Einstellungen für **Sicheres Wake On LAN (WOL)** definieren Sie in einer Richtlinie des Typs **Spezifische Computereinstellungen**.

28.1 Sicheres Wake on LAN (WOL): Beispiel

Das SW-Rollout-Team informiert den SafeGuard Enterprise Sicherheitsbeauftragten (SO) über einen geplanten SW-Rollout für den 25. September 2014 zwischen 03.00 und 06.00 Uhr. Es sind 2 Neustarts notwendig. Der lokale Software Rollout Agent muss sich an Windows anmelden können.

Im SafeGuard Management Center, erstellt der Sicherheitsbeauftragter eine Richtlinie vom Typ **Spezifische Computereinstellungen** mit den folgenden Einstellung und ordnet Sie den relevanten Endpoints zu.

Richtlinieneinstellung	Wert
Anzahl der automatischen Anmeldungen (0 = kein WOL)	5
Anmeldung an Windows während WOL erlaubt	Ja
Beginn des Zeitfensters für externen WOL Start	24.Sept. 2014, 12:00
Ende des Zeitfensters für externen WOL Start	25.Sept. 2014, 06:00

Weitere Informationen zu den einzelnen Einstellungen finden Sie unter Spezifische Computereinstellungen - Grundeinstellungen (Seite 156).

Da die Anzahl an automatischen Anmeldungen auf 5 eingestellt ist, startet der Endpoint 5 mal ohne Authentisierung durch die SafeGuard POA.

Hinweis: Wir empfehlen, für Wake on LAN immer **drei Neustarts mehr als notwendig** zu erlauben, um unvorhergesehene Probleme zu umgehen.

Das Zeitintervall setzt der SO auf 12:00 Uhr mittags auf den Tag vor dem SW-Roll-Out. Somit kann das Scheduling-Skript SGMCMDIntn.exe rechtzeitig starten und WOL ist spätestens am 25.09 um 03:00 Uhr gestartet.

Das SW-Roll-Out-Team erstellt 2 Kommandos für das Scheduling-Skript:

- Starte am 24. Sept. 2014, 12.15 Uhr SGMCMDIntn.exe -WOLstart
- Starte am 26. Sept. 2014, 09.00 Uhr SGMCMDIntn.exe -WOLstop

Das SW-Rollout-Skript wird auf den 25.09.2014, 03.00 Uhr datiert. Am Ende des Skripts kann WOL explizit wieder deaktiviert werden mit SGMCMDIntn.exe -WOLstop.

Alle Endpoints, die sich bis zum 24.Sept. 2014 anmelden und mit den Roll-out Servern in Verbindung treten, erhalten die neue Richtlinie und die Scheduling-Kommandos.

Jeder Endpoint, auf dem der Scheduler zwischen dem 24. Sept. 2014,12:00 Uhr und dem 26. Sept. 2014, 09:00 Uhr das Kommando SGMCMDIntn -WOLstart auslöst, fällt in das obige WOL-Zeitintervall und aktiviert demzufolge Wake on LAN.

29 Recovery-Optionen

Für Recovery-Vorgänge bietet SafeGuard Enterprise verschiedene Optionen, die auf unterschiedliche Szenarien zugeschnitten sind:

- **Recovery für die Anmeldung mit Local Self Help**

  Local Self Help ermöglicht es Benutzern, die Ihr Kennwort vergessen haben, sich selbständig und ohne Unterstützung des Helpdesk an ihrem Computer anzumelden. So erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, müssen sie lediglich eine bestimmte Anzahl an vordefinierten Fragen in der SafeGuard Power-on Authentication beantworten.

  Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Recovery-Vorgänge, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

  Weitere Informationen finden Sie unter Recovery mit Local Self Help (Seite 235).

- **Recovery mit Challenge/Response**

  Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System, das Benutzer unterstützt, die sich nicht mehr an ihrem Computer anmelden oder nicht mehr auf verschlüsselte Daten zugreifen können. Während eines Challenge/Response-Verfahrens übermittelt der Benutzer einen auf dem Endpoint erzeugten Challenge-Code an den Helpdesk-Beauftragten. Dieser erzeugt auf der Grundlage des Challenge-Codes einen Response-Code, der den Benutzer zum Ausführen einer bestimmten Aktion auf dem Computer berechtigt.

  Mit Recovery über Challenge/Response bietet SafeGuard Enterprise verschiedene Workflows für typische Recovery-Szenarien, für die die Unterstützung durch einen Helpdesk erforderlich ist.

  Weitere Informationen finden Sie unter Recovery mit Challenge/Response (Seite 239).

- **System-Recovery für die Sophos SafeGuard Festplattenverschlüsselung**

  SafeGuard Enterprise bietet verschiedene Methoden und Tools für Recovery-Vorgänge in Bezug auf wichtige System- und SafeGuard Enterprise Komponenten, z. B.:

  - Beschädigter MBR
  - SafeGuard Enterprise Kernel-Probleme
  - Probleme in Bezug auf Volume-Zugriff
  - Windows Bootprobleme

Weitere Informationen finden Sie unter System-Recovery für die Sophos SafeGuard Festplattenverschlüsselung (Seite 256).

29.1 Recovery mit Local Self Help

Hinweis: Local Self Help ist nur für Windows 7 Endpoints mit SafeGuard Power-on Authentication (POA) verfügbar.

Über Local Self Help können sich Benutzer, die Ihr Kennwort vergessen haben, ohne Unterstützung des Helpdesks wieder an ihrem Computer anmelden. Local Self Help reduziert die Anzahl an Helpdesk-Anforderungen für Recovery-Vorgänge, die die Anmeldung betreffen. Helpdesk-Mitarbeitern werden somit Routine-Aufgaben abgenommen und sie können sich auf komplexere Support-Anforderungen konzentrieren.

Mit Local Self Help erhalten Benutzer auch in Situationen, in denen sie keine Telefon- oder Netzwerkverbindung und somit auch kein Challenge/Response-Verfahren nutzen können (z. B. an Bord eines Flugzeugs), wieder Zugang zu ihrem Computer. Um sich anzumelden, muss der Benutzer lediglich eine bestimmte Anzahl an vordefinierten Fragen in der SafeGuard Power-on Authentication beantworten.

Die zu beantwortenden Fragen können Sie als zuständiger Sicherheitsbeauftragter zentral vordefinieren und per Richtlinie an die Endpoints verteilen. Als Vorlage bieten wir Ihnen ein vordefiniertes Fragenthema an. Sie können dieses Fragenthema unverändert verwenden oder es bearbeiten. Sie können die Benutzer auch per Richtlinie berechtigen, selbst Fragen zu definieren.

Wenn Local Self Help per Richtlinie aktiviert ist, steht den Endbenutzern ein Local Self Help Assistent zur Verfügung, der sie bei der ersten Beantwortung und bei der Bearbeitung von Fragen unterstützt.

Detaillierte Informationen zu Local Self Help auf dem Endpoint finden Sie in der *SafeGuard Enterprise Benutzerhilfe* im Kapitel *Recovery mit Local Self Help*.

29.1.1 Definieren der Parameter für Local Self Help in einer Richtlinie

Die Einstellungen für Local Self Help definieren Sie in einer Richtlinie vom Typ **Allgemeine Einstellungen** unter **Recovery für die Anmeldung** - **Local Self Help**. Hier aktivieren Sie die Funktion zur Benutzung auf den Endpoints und legen weitere Berechtigungen und Parameter fest.

Local Self Help aktivieren

Um die Funktion Local Self Help für die Benutzung auf Endpoints zu aktivieren, wählen Sie im Feld **Local Self Help aktivieren** die Einstellung **Ja**.

Nach dem Wirksamwerden der Richtlinie auf den Endpoints sind die Benutzer aufgrund dieser Einstellung berechtigt, Local Self Help für Recovery-Vorgänge, die die Anmeldung betreffen, zu benutzen. Hierzu müssen die Benutzer die Funktion auf Ihrem Computer durch Beantwortung einer festgelegten Anzahl der erhaltenen Fragen oder durch Erstellung und Beantwortung eigener Fragen (je nach Berechtigung) aktivieren.

Nach dem Erhalt der Richtlinie und dem Neustart des Computers steht den Benutzern dafür der Local Self Help Assistent über das System Tray Icon in der Windows-Taskleiste zur Verfügung.

Konfigurieren der Funktion Local Self Help

Sie können folgende Optionen für Local Self Help in einer Richtlinie des Typs **Allgemeine Einstellungen** definieren.

- **Mindestlänge der Antwort**

  Legen Sie die Mindestlänge der Antworten in Zeichen fest. Die Standardeinstellung ist **1**.

- **Willkommenstext unter Windows**

  Sie können einen individuellen Informationstext angeben, der beim Starten des Local Self Help Assistenten auf dem Endpoint im ersten Dialog angezeigt werden soll. Dieser Text muss zuvor erstellt und registriert werden.

- **Benutzer dürfen eigene Fragen festlegen**

  Für die Hinterlegung der Fragen und Antworten für Local Self Help gibt es folgende Möglichkeiten:

  - Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind nicht dazu berechtigt, eigene Fragen zu definieren.

  - Sie definieren als Sicherheitsbeauftragter die Fragen und verteilen Sie an die Benutzer. Die Benutzer sind dazu berechtigt, zusätzlich eigene Fragen zu definieren. Bei der Beantwortung der für die Aktivierung von Local Self Help notwendigen Mindestanzahl an Fragen können die Benutzer zwischen vorgegebenen und eigenen Fragen wählen oder eine Kombination aus beiden verwenden.
  - Sie berechtigen die Benutzer dazu, eigene Fragen zu definieren und geben keine vordefinierten Fragen vor. Die Benutzer aktivieren Local Self Help durch Definition und Beantwortung eigener Fragen.

Um die Benutzer dazu zu berechtigen, eigene Fragen zu definieren, wählen Sie im Feld **Benutzer dürfen eigene Fragen festlegen** die Einstellung **Ja**.

29.1.2 Definieren von Fragen

Voraussetzung dafür, dass Local Self Help auf dem Endpoint verwendet werden kann, ist die Hinterlegung einer vordefinierten Anzahl an Fragen. Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie festlegen, wie viele Fragen Benutzer beantworten müssen, um Local Self Help auf den Endpoints zu aktivieren. Sie können auch festlegen, wie viele Fragen in der SafeGuard POA per Zufallsprinzip ausgewählt werden. Um sich über Local Self Help an der SafeGuard Power-on Authentication anzumelden, muss der Benutzer alle in der POA angezeigten Fragen korrekt beantworten.

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie Local Self Help Fragen im SafeGuard Management Center registrieren und bearbeiten.

Hinweis:

Nicht alle Zeichen, die in Windows eingegeben werden können, können von der SafeGuard POA verarbeitet werden. Hebräische oder arabische Zeichen können z. B. nicht verwendet werden.

29.1.3 Festlegen der Anzahl an zu beantwortenden Fragen

Sie können die Anzahl an Fragen, die während der Konfiguration von Local Self Help und in der SafeGuard POA beantwortet werden müssen, festlegen.

1. Markieren Sie im **Richtlinien** Navigationsbereich den Eintrag **Local Self Help Fragen**.
2. Im Aktionsbereich können Sie unter **Local Self Help Parameter** zwei verschiedene Werte für die Anzahl an Local Self Help Fragen festlegen:

   a) Geben Sie im Feld **Mindestanzahl der verfügbaren Fragen/Antworten** an, wie viele Fragen die Benutzer im Local Self Help Assistenten beantworten müssen, um Local Self Help auf den Endpoints zu aktivieren.

      Die hier angegebene Anzahl an Fragen muss auf dem Endpoint mit den entsprechenden Antworten verfügbar sein, damit Local Self Help aktiv ist.

   b) Geben Sie im Feld **Anzahl der in der POA gestellten Fragen** an, wie viele Fragen die Benutzer in der SafeGuard POA beantworten müssen, wenn Sie sich mit Local Self Help anmelden.

      Die in der SafeGuard POA angezeigten Fragen werden per Zufallsprinzip aus den Fragen, die der Benutzer im Local Self Help Assistenten beantwortet hat, ausgewählt.

   Der im Feld **Mindestanzahl der verfügbaren Fragen/Antworten** angegebene Wert muss höher sein als der Wert im Feld **Anzahl der in der POA gestellten Fragen**. Ist dies nicht der Fall, so wird beim Speichern Ihrer Änderungen eine Fehlermeldung angezeigt.

   Die Felder haben folgende Standardwerte:

   - **Mindestanzahl der verfügbaren Fragen/Antworten:** 10
   - **Anzahl der in der POA gestellten Fragen:** 5

3. Speichern Sie Ihre Änderungen in der Datenbank.

Die festgelegten Werte für die Fragenanzahl gelten für die Local Self Help Konfiguration, die an die Endpoints übertragen wird.

29.1.4 Verwenden der Vorlage

Für Local Self Help ist ein vordefiniertes Fragenthema verfügbar. Sie finden dieses Fragenthema im SafeGuard Management Center unter **Local Self Help Fragen**.

Sie können das vordefinierte Fragenthema unverändert verwenden, bearbeiten oder löschen.

29.1.5 Import von Fragenthemen

Mit dem Importvorgang können Sie Ihre eigenen als .XML-Dateien angelegten Fragenlisten importieren.

1. Erstellen Sie ein neues Fragenthema (siehe Erstellen eines neuen Fragenthemas und Hinzufügen von Fragen (Seite 238)).
2. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
3. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Importieren**.

4. Wählen Sie das Verzeichnis, in dem das Fragenthema abgelegt ist, sowie das gewünschte Fragenthema und klicken Sie auf **Öffnen**.

Die importierten Fragen werden im Arbeitsbereich angezeigt. Sie können das Fragenthema nun unverändert speichern oder bearbeiten.

29.1.6 Erstellen eines neuen Fragenthemas und Hinzufügen von Fragen

Sie können neue Fragenthemen zu unterschiedlichen Themenbereichen erstellen. Somit können Sie Benutzern mehrere Fragenthemen zur Verfügung stellen, aus denen sie das für sie am besten geeignete Thema auswählen können.

1. Markieren Sie im **Richtlinien** Navigationsbereich den Eintrag **Local Self Help Fragen**.
2. Klicken Sie mit der rechten Maustaste auf **Local Self Help Fragen** und wählen Sie **Neu > Fragenthema**.
3. Geben Sie einen Namen für das Fragenthema ein und klicken Sie auf **OK**.
4. Markieren Sie im **Richtlinien** Navigationsbereich das neue Fragenthema unter **Local Self Help Fragen**.
5. Klicken Sie im Arbeitsbereich mit der rechten Maustaste. Das Kontextmenü für das Fragenthema wird geöffnet. Wählen Sie **Hinzufügen** im Kontextmenü.

   Eine neue Fragenzeile wird hinzugefügt.

6. Geben Sie Ihre Frage ein und drücken Sie **Enter**. Um weitere Fragen hinzuzufügen, wiederholen Sie diesen Vorgang.
7. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern** Symbol in der Symbolleiste klicken.

Ihr Fragenthema ist registriert. Es wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoints aktiviert wird, automatisch mitgegeben.

29.1.7 Bearbeiten von Fragenthemen

1. Markieren Sie das gewünschte Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich.
2. Sie können nun Fragen hinzufügen, ändern oder löschen.
   - Um Fragen hinzuzufügen, klicken Sie im Arbeitsbereich mit der rechten Maustaste, um das Kontextmenü anzuzeigen. Klicken Sie im Kontextmenü auf **Hinzufügen**. Der Fragenliste wird eine neue Zeile hinzugefügt. Geben Sie Ihre Frage auf der Zeile ein.
   - Um Fragen zu ändern, klicken Sie auf den Fragentext im Arbeitsbereich. Bei der gewählten Frage wird ein Stiftsymbol angezeigt. Geben Sie auf der Fragenzeile Ihre Änderungen ein.
   - Um Fragen zu löschen, markieren Sie die gewünschte Frage durch Klicken auf das graue Kästchen zu Beginn der Fragenzeile im Arbeitsbereich und wählen Sie im Kontextmenü des Frageneintrags **Entfernen**.
3. Speichern Sie Ihre Änderungen, indem Sie auf das **Speichern** Symbol in der Symbolleiste klicken.

Ihr geändertes Fragenthema ist registriert. Es wird der Richtlinie vom Typ **Allgemeine Einstellungen**, über die Local Self Help auf den Endpoints aktiviert wird, mitgegeben.

29.1.8 Löschen von Fragenthemen

Um ein Fragenthema zu löschen, klicken Sie mit der rechten Maustaste auf das Fragenthema unter **Local Self Help Fragen** im **Richtlinien** Navigationsbereich und wählen Sie **Löschen**.

Hinweis: Wenn Sie ein Fragenthema löschen, nachdem die Benutzer bereits Fragen aus diesem Thema zur Aktivierung von Local Self Help auf ihren Computern beantwortet haben, werden die Antworten der Benutzer ungültig, da die Fragen nicht mehr vorhanden sind.

29.1.9 Registrieren von Willkommenstexten

Sie können einen Willkommenstext registrieren, der im ersten Dialog des Local Self Help Assistenten angezeigt werden soll.

Die Textdateien mit den gewünschten Informationen müssen erstellt werden, bevor sie im SafeGuard Management Center registriert werden können. Die maximale Dateigröße für Informationstexte beträgt 50 KB. SafeGuard Enterprise verwendet nur Unicode UTF-16 kodierte Texte. Wenn Sie die Textdateien nicht in diesem Format erstellen, werden sie bei der Registrierung automatisch in dieses Format konvertiert.

1. Klicken Sie im **Richtlinien**-Navigationsbereich mit der rechten Maustaste auf **Texte** und wählen Sie **Neu > Text**.
2. Geben Sie unter **Textelementname** einen Namen für den anzeigenden Text ein.
3. Klicken Sie auf **[...]** um die zuvor erstellte Textdatei auszuwählen. Wenn eine Konvertierung notwendig ist, wird eine entsprechende Meldung angezeigt.
4. Klicken Sie auf **OK**.

Das neue Textelement wird als Unterknoten des Eintrags **Texte** im **Richtlinien**-Navigationsbereich angezeigt. Ist ein Textelement markiert, wird sein Inhalt im Aktionsbereich auf der rechten Seite angezeigt. Das Textelement kann jetzt beim Erstellen von Richtlinien ausgewählt werden.

Um weitere Textelemente zu registrieren, gehen Sie wie beschrieben vor. Alle registrierten Textelemente werden als Unterknoten angezeigt.

29.2 Recovery mit Challenge/Response

Zur Optimierung von Workflows im Unternehmen und zur Reduzierung von Helpdesk-Kosten bietet Sophos SafeGuard eine Challenge/Response Recovery-Lösung. Mit einem benutzerfreundlichen Challenge/Response-Verfahren unterstützt SafeGuard Enterprise Benutzer, die sich an ihrem Computer nicht mehr anmelden oder nicht auf verschlüsselte Daten zugreifen können.

Diese Funktionalität ist im SafeGuard Enterprise Management Center in Form eines **Recovery-Assistenten** integriert.

Nutzen und Vorteile des Challenge/Response-Verfahrens

Das Challenge/Response-Verfahren ist ein sicheres und effizientes Recovery-System.

- Während des gesamten Vorgangs werden keine vertraulichen Daten in unverschlüsselter Form ausgetauscht.

- Informationen, die unberechtigte Dritte durch Mitverfolgen dieses Vorgangs erhalten könnten, lassen sich weder zu einem späteren Zeitpunkt noch auf anderen Geräten verwenden.
- Für den Computer, auf den zugegriffen werden soll, muss während des Vorgangs keine Online-Netzwerkverbindung bestehen. Der Response Code-Assistent für den Helpdesk läuft auch auf einem Standalone-Endpoint ohne Verbindung zum SafeGuard Enterprise Server. Eine komplexe Infrastruktur ist nicht notwendig.
- Der Benutzer kann schnell wieder mit dem Computer arbeiten. Es gehen keine verschlüsselten Daten verloren, nur weil der Benutzer das Kennwort vergessen hat.

Typische Notfälle, in denen Hilfe beim Helpdesk angefordert wird

- Ein Benutzer hat sein Kennwort für die Anmeldung vergessen. Der Computer ist gesperrt.
- Ein Benutzer hat seinen Token/seine Smartcard vergessen oder verloren.
- Der lokale Cache der SafeGuard Power-on Authentication ist teilweise beschädigt.
- Ein Benutzer ist krank oder im Urlaub und ein Kollege muss auf die Daten auf dem Computer zugreifen.
- Ein Benutzer möchte auf ein Volume zugreifen, das mit einem Schlüssel verschlüsselt ist, der auf dem Computer nicht verfügbar ist.

SafeGuard Enterprise bietet für diese typischen Notfälle unterschiedliche Recovery-Workflows, die dem Benutzer wieder den Zugang zu seinem Computer ermöglichen.

29.2.1 Challenge/Response Workflow

Das Challenge/Response-Verfahren basiert auf zwei Komponenten:

- Endpoint, auf dem der Challenge Code erzeugt wird.
- SafeGuard Management Center, in dem Sie als Helpdesk-Beauftragter mit ausreichenden Rechten einen Response-Code erstellen, der den Benutzer zur Ausführung der angeforderten Aktion auf dem Computer berechtigt.

  Hinweis: Für ein Challenge/Response-Verfahren benötigen Sie das Zugriffsrecht **Voller Zugriff** für die beteiligten Computer/Benutzer.

1. Der Benutzer fordert auf dem Endpoint einen Challenge-Code an. Je nach Recovery-Typ wird der Challenge-Code in der SafeGuard Power-on Authentication oder über das KeyRecovery Tool angefordert.

   Es wird ein Challenge-Code aus Ziffern und Buchstaben erzeugt und angezeigt.
2. Der Benutzer wendet sich an den Helpdesk und übermittelt die notwendige Identifizierungsinformationen sowie den Challenge-Code.
3. Der Helpdesk-Beauftragte startet den Recovery-Assistenten im SafeGuard Management Center.

4. Der Helpdesk-Beauftragte wählt den entsprechenden Recovery-Typ, bestätigt die Identifikationsinformationen sowie den Challenge-Code und wählt die gewünschte Recovery-Aktion aus.

   Ein Response-Code in Form einer ASCII-Zeichenfolge wird generiert und angezeigt.

5. Der Helpdesk übermittelt den Response-Code per Telefon oder Text-Mitteilung an den Benutzer.
6. Der Benutzer gibt den Response-Code ein. Je nach Recovery-Typ erfolgt dies in der SafeGuard POA oder über das KeyRecovery Tool.

   Der Benutzer kann die autorisierte Aktion, z. B. Rücksetzen des Kennworts, ausführen und wieder mit dem Computer arbeiten.

29.2.2 Wann muss der Benutzer sein Kennwort ändern?

Im Rahmen eines SafeGuard Enterprise Recovery-Vorgangs muss der Benutzer u. U. sein Windows-Kennwort ändern. Die folgende Tabelle zeigt, wann es erforderlich ist, das Kennwort zu ändern. Die ersten vier Spalten zeigen spezifische Bedingungen, die während des Challenge/Response-Verfahrens auftreten können. Die letzte Spalte gibt basierend auf den Bedingungen aus den ersten vier Spalten an, ob der Benutzer sein Kennwort ändern muss.

Bedingung: C/R mit Benutzeranmeldung und Anzeige des Kennworts	Bedingung: C/R mit Benutzeranmeldung	Bedingung: Domänen-Controller verfügbar	Bedingung: Option zur Kennwortanzeige vom Benutzer abgelehnt	Ergebnis: Benutzer muss sein Windows-Kennwort ändern
Ja	Ja	Ja	Nein	**Nein**
Ja	Ja	Ja	Ja	**Ja**
Ja	Ja	Nein	Ja	**Nein**
Nein	Ja	Ja	entf.	**Ja**
Nein	Ja	Nein	entf.	**Nein**
Nein	Nein	Nein	entf.	**Nein**

29.2.3 Starten des Recovery-Assistenten

Damit Sie in der Lage sind, ein Recovery-Verfahren auszuführen, stellen Sie sicher, dass Sie über die erforderlichen Rechte und Berechtigungen verfügen.

1. Melden Sie sich am SafeGuard Management Center an.
2. Klicken Sie auf **Extras > Recovery** in der Menüleiste.

Der SafeGuard **Recovery-Assistent** wird gestartet. Sie können wählen, welchen Recovery-Typ Sie verwenden möchten.

29.2.4 Recovery-Typen

Wählen Sie den Recovery-Typ, den Sie verwenden möchten. Folgende Recovery-Typen stehen zur Verfügung:

- **SafeGuard Enterprise Clients (managed)**

  Challenge/Response für zentral durch das SafeGuard Management Center verwaltete Endpoints. Sie werden im Bereich **Benutzer und Computer** des SafeGuard Management Centers angezeigt.

- **Virtuelle Clients**

  In komplexen Recovery-Situationen, zum Beispiel wenn die SafeGuard POA beschädigt ist, lässt sich der Zugriff auf verschlüsselte Daten auf einfache Art und Weise mit Challenge/Response wieder herstellen. In diesem Fall werden spezifische Dateien mit der Bezeichnung virtuelle Clients verwendet. Diese Art von Dateien ist sowohl für zentral verwaltete Computer als auch für Standalone-Endpoints verfügbar.

- **Sophos SafeGuard Clients (Standalone)**

  Challenge/Response für Standalone-Endpoints Diese Endpoints haben nie eine Verbindung zum SafeGuard Enterprise Server. Die erforderlichen Recovery-Informationen basieren auf der Schlüssel-Recovery-Datei. Diese Datei wird auf jedem Endpoint während der Installation der Sophos SafeGuard Verschlüsselungssoftware erzeugt. Um in diesem Fall Challenge/Response zur Verfügung zu stellen, muss die Schlüssel-Recovery-Datei dem SafeGuard Enterprise Helpdesk zur Verfügung stehen, zum Beispiel auf einer Netzwerkfreigabe.

Hinweis: Darüber hinaus steht das Recovery-Verfahren Local Self Help zur Verfügung, für das keine Unterstützung durch den Helpdesk benötigt wird.

29.2.5 Challenge/Response für SafeGuard Enterprise Clients (Managed)

SafeGuard Enterprise bietet ein Recovery-Verfahren für in der Datenbank registrierte Endpoints für verschiedene Recovery-Szenarien, z. B. Kennwort-Recovery.

Das Challenge/Response-Verfahren wird sowohl für native SafeGuard Enterprise Computer als auch für mit BitLocker verschlüsselte Endpoints unterstützt. Das System ermittelt den Computertyp dynamisch. Der Recovery-Workflow wird dementsprechend angepasst.

29.2.5.1 Recovery-Aktionen für SafeGuard Enterprise Clients

Der Recovery Workflow richtet sich danach, für welchen Typ von Endpoint das Recovery-Verfahren angefordert wird.

Hinweis: Für mit BitLocker verschlüsselte Computer steht als Recovery-Aktion nur die Wiederherstellung des Schlüssels, der für die Verschlüsselung eines spezifischen Volumes verwendet wurde, zur Verfügung. Eine Recovery-Aktion für Kennwörter ist nicht verfügbar.

29.2.5.1.1 Wiederherstellen des Kennworts auf SafeGuard POA-Ebene

Eines der am häufigsten auftretenden Recovery-Szenarien besteht darin, dass Benutzer ihr Kennwort vergessen haben. SafeGuard Enterprise wird standardmäßig mit aktivierter SafeGuard Power-on Authentication (POA) installiert. Das SafeGuard POA-Kennwort, mit dem auf den Computer zugegriffen wird, ist identisch mit dem Windows-Kennwort.

Wenn der Benutzer das Kennwort auf der SafeGuard POA-Ebene vergessen hat, generiert der Helpdesk-Beauftragte eine Response mit der Option **SGN Client mit Benutzeranmeldung booten**, ohne das Benutzerkennwort anzuzeigen. In diesem Fall startet der Computer jedoch nach der Eingabe des Response-Codes bis zum Betriebssystem. Der Benutzer muss das Kennwort auf Windows-Ebene ändern, vorausgesetzt, die Domäne ist erreichbar. Danach kann der Benutzer sich sowohl an Windows als auch an der SafeGuard Power-on Authentication mit dem neuen Kennwort anmelden.

29.2.5.1.2 Best Practice für das Wiederherstellen des Kennworts auf SafeGuard POA-Ebene

Wir empfehlen, folgende Methoden anzuwenden, wenn der Benutzer sein Kennwort vergessen hat, um zu vermeiden, dass das Kennwort zentral zurückgesetzt werden muss:

- **Benutzen Sie Local Self Help.**

  Mit Recovery über Local Self Help kann sich der Benutzer das aktuelle Kennwort anzeigen lassen und dieses weiterhin benutzen, ohne es zurücksetzen zu müssen. Bei der Benutzung von Local Self Help ist außerdem keine Unterstützung durch den Helpdesk erforderlich.

- **Bei Anwendung von Challenge/Response für SafeGuard Enterprise Clients (Managed):**

  Wir empfehlen, das Kennwort vor dem Challenge/Response-Verfahren nicht zentral im Active Directory zurückzusetzen. Dadurch wird gewährleistet, dass das Kennwort zwischen Windows und SafeGuard Enterprise synchron bleibt. Stellen Sie sicher, dass der Windows-Helpdesk entsprechend informiert ist.

Erzeugen Sie als SafeGuard Enterprise Helpdesk-Beauftragter eine Response für das **Booten des SGN Clients mit Benutzeranmeldung** mit der Option **Benutzerkennwort anzeigen**. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Der Benutzer kann mit dem alten Kennwort weiterarbeiten und dieses später nach Wunsch lokal ändern.

29.2.5.1.3 Anzeigen des Benutzerkennworts

SafeGuard Enterprise bietet Benutzern die Möglichkeit, sich ihr Kennwort während des Challenge/Response-Verfahrens anzeigen zu lassen. Dies bietet den Vorteil, dass das Kennwort nicht im Active Directory geändert werden muss. Diese Option ist verfügbar, wenn die Anforderung **SGN Client mit Benutzeranmeldung booten** gestellt wird.

29.2.5.1.4 Ein anderer Benutzer muss den durch SafeGuard Enterprise geschützten Endpoint starten

In diesem Fall startet der Benutzer, der Zugriff benötigt, den Endpoint und gibt seinen Benutzernamen ein. Der Benutzer fordert dann eine Challenge an. Der SafeGuard Helpdesk generiert eine Response vom Typ **SGN Client mit Benutzeranmeldung booten** mit aktivierter **durchgehender Anmeldung an Windows**. Der Benutzer wird angemeldet und kann den Computer benutzen.

29.2.5.1.5 Wiederherstellen des SafeGuard Enterprise Policy Cache

Diese Aktion wird notwendig, wenn der SafeGuard Policy Cache beschädigt ist. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien gespeichert. Standardmäßig ist Recovery für die Anmeldung bei einem beschädigten Local Cache deaktiviert. Er wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist für das Reparieren des Local Cache kein Challenge/Response-Verfahren erforderlich. Wenn der Local Cache mit einem Challenge/Response-Verfahren repariert werden soll, können Sie den Recovery-Vorgang per Richtlinie aktivieren. In diesem Fall wird der Benutzer bei einem beschädigten Local Cache automatisch dazu aufgefordert, ein Challenge/Response-Verfahren zu starten.

29.2.5.1.6 SafeGuard Data Exchange: Recovery-Vorgänge bei vergessenem Kennwort

SafeGuard Data Exchange ohne Device Encryption bietet für den Fall, dass der Benutzer sein Kennwort vergessen hat, keinen Recovery-Vorgang über Challenge/Response. In diesem Fall müssen Sie das Kennwort im Active Directory ändern. Melden Sie sich ohne Sophos Credential Provider am Endpoint an und stellen Sie die Benutzerkonfiguration auf dem Endpoint wieder her.

29.2.5.2 Response für SafeGuard Enterprise Clients

1. Wählen Sie auf der **Recovery-Typ** Seite die Option **SafeGuard Enterprise Client (Managed)**.
2. Wählen Sie unter **Domäne** die gewünschte Domäne aus der Liste.
3. Geben Sie unter **Computer** den gewünschten Computernamen ein oder wählen Sie ihn aus. Hierzu gibt es mehrere Möglichkeiten:
   - Um einen Namen auszuwählen, klicken Sie auf **[...]**. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird auf der Seite **Recovery-Typ** angezeigt.
   - Geben Sie den Kurznamen des Computers direkt in das Feld ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     `CN=Desktop1,OU=Development,OU=Headquarter,DC=Sophos,DC=edu`
4. Klicken Sie auf **Weiter**.
5. Wählen Sie die Domäne des Benutzers.
6. Geben Sie den Benutzernamen ein. Hierfür gibt es mehrere Möglichkeiten:
   - Um den Benutzernamen auszuwählen, klicken Sie auf **[...]** im Abschnitt **Benutzer-Information** des Dialogs **Recovery für die Anmeldung**. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit Benutzernamen wird angezeigt. Wählen Sie den gewünschten Namen und klicken Sie auf **OK**. Der Benutzername wird auf der Seite **Recovery-Typ** angezeigt.
   - Geben Sie den Benutzernamen direkt ein. Stellen Sie sicher, dass der Name korrekt geschrieben ist.
7. Klicken Sie auf **Weiter**.

   Eine Seite für die Eingabe des Challenge-Codes wird angezeigt.
8. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültige Challenge** angezeigt.
9. Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom SafeGuard Enterprise Client angeforderte Aktion sowie die möglichen Recovery-Aktionen auf dem Client angezeigt. Die möglichen Response-Aktionen richten sich nach den Aktionen, die auf Client-Seite beim Aufrufen der Challenge angefordert wurden. Wenn auf Client-Seite zum Beispiel **Crypto Token erforderlich** angefordert wurde, stehen für die Response die Aktionen **SGN Client mit Benutzeranmeldung booten** und **SGN Client ohne Benutzeranmeldung booten** zur Verfügung.
10. Wählen Sie die Aktion, die der Benutzer ausführen soll.

11. Wenn Sie **SGN Client mit Benutzeranmeldung booten** ausgewählt haben, können Sie zusätzlich auch die Option **Benutzerkennwort anzeigen** wählen, um das Kennwort auf dem Zielcomputer anzeigen zu lassen.
12. Klicken Sie auf **Weiter**.
13. Es wird ein Response-Code erzeugt. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann nun den Response-Code auf dem Endpoint eingeben und die autorisierte Aktion durchführen.

29.2.6 Challenge/Response mit virtuellen Clients

Mit Recovery über Challenge/Response mit virtuellen Clients bietet SafeGuard Enterprise ein Recovery-Verfahren für verschlüsselte Volumes in komplexen Notfallsituationen, z. B., wenn die SafeGuard POA beschädigt ist. Dieses Verfahren lässt sich sowohl auf zentral verwaltete Endpoints als auch auf Standalone Endoints anwenden.

Hinweis: Recovery mit virtuellen Clients sollte nur in komplexen Notfallsituationen angewendet werden. Wenn zum Beispiel nur ein Schlüssel für die Wiederherstellung eines Volumes fehlt, ist es am besten, den fehlenden Schlüssel dem Schlüsselbund des entsprechenden Benutzers zuzuweisen, um den Zugriff auf das Volume zu ermöglichen.

29.2.6.1 Recovery Workflow mit virtuellen Clients

Über folgenden allgemeinen Workflow lässt sich der Zugang zum verschlüsselten Endpoint wiederherstellen:

1. Sie erhalten die SafeGuard Enterprise Recovery Disk vom technischen Support.

   Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen SafeGuard Enterprise Filter-Treibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie unter: http://www.sophos.com/de-de/support/knowledgebase/108805.aspx.

2. Erstellen Sie den virtuellen Client im SafeGuard Management Center (siehe Erstellen von virtuellen Clients (Seite 81)).

3. Exportieren Sie den virtuellen Client in eine Datei (sieheExportieren von virtuellen Clients (Seite 81)).

4. Optional können Sie mehrere Schlüssel für virtuelle Clients in eine Datei exportieren (siehe Anlegen und Exportieren von Schlüsseldateien für den Recovery-Vorgang (Seite 81)).

5. Booten Sie den Endpoint von der Recovery Disk.

6. Importieren Sie die Datei mit dem virtuellen Client in das KeyRecovery Tool.

7. Starten Sie die Challenge im KeyRecovery Tool.

8. Bestätigen Sie den virtuellen Client im SafeGuard Management Center.

9. Wählen Sie die erforderliche Recovery-Aktion.

10. Geben Sie den Challenge-Code im SafeGuard Management Center ein.

11. Generieren Sie den Response-Code im SafeGuard Management Center.

12. Geben Sie den Response-Code im KeyRecovery Tool ein.

Auf den Computer kann wieder zugegriffen werden.

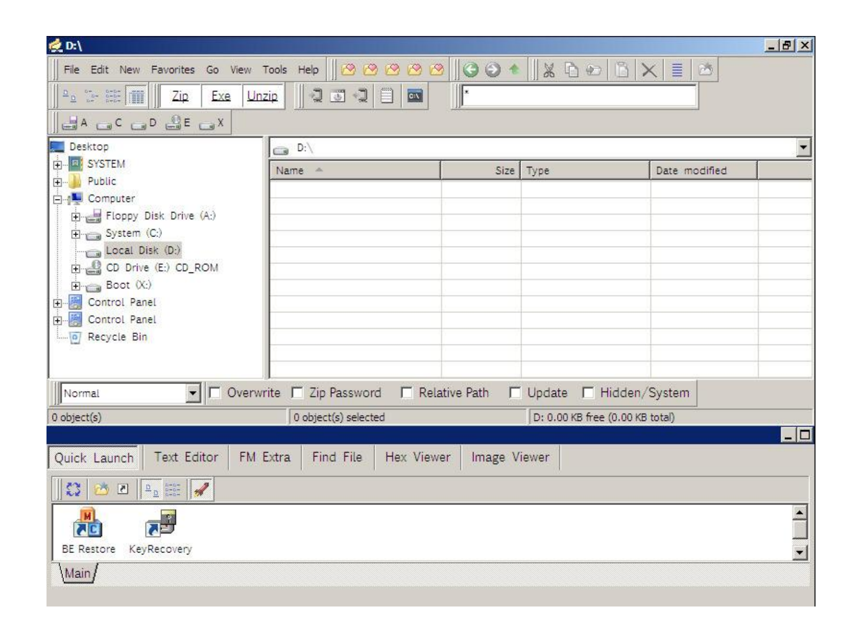
29.2.6.2 Booten des Computers von der Recovery Disk.

Voraussetzung: Stellen Sie sicher, dass die Boot-Reihenfolge im BIOS das Booten von CD erlaubt.

1. Fordern Sie vom technischen Support von Sophos die SafeGuard Enterprise Windows PE Disk an.

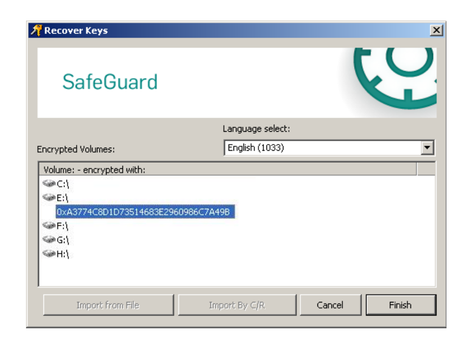
   Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen SafeGuard Enterprise Filter-Treibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/108805.aspx.

2. Legen Sie auf dem Endpoint die Recovery Disk ein und starten Sie den Computer. Der integrierte Dateimanager wird geöffnet. Hier sehen Sie auf einen Blick die bereitgestellten Volumes und Laufwerke.



   Der Inhalt des verschlüsselten Laufwerks ist im Dateimanager nicht sichtbar. In den Eigenschaften des verschlüsselten Laufwerks werden weder das Dateisystem, noch die Kapazität sowie der verwendete/freie Speicherplatz angegeben.

3. Klicken Sie unten im Bereich **Quick Launch** des Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt die Schlüssel-ID verschlüsselter Laufwerke.



4. Suchen Sie nach der Schlüssel-ID des Laufwerks, auf das Sie zugreifen möchten. Die Schlüssel-ID wird später abgefragt.

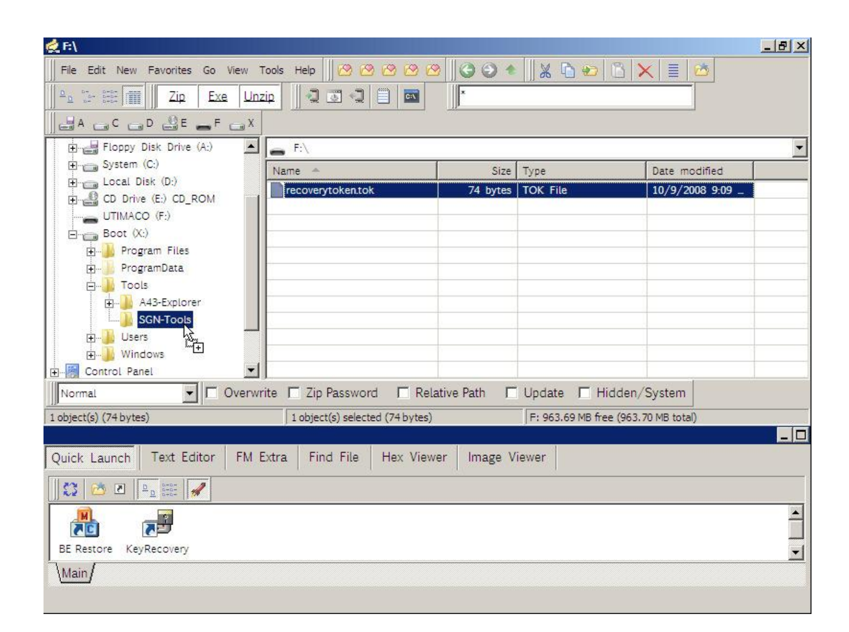
Im nächsten Schritt importieren Sie den virtuellen Client in das Key Recovery Tool.

29.2.6.3 Import des virtuellen Client in das KeyRecovery Tool

Voraussetzung:

- Der Computer wurde von der Recovery Disk gebootet.
- Stellen Sie sicher, dass das USB-Laufwerk mit der Datei **`recoverytoken.tok`** erfolgreich bereitgestellt wurde.

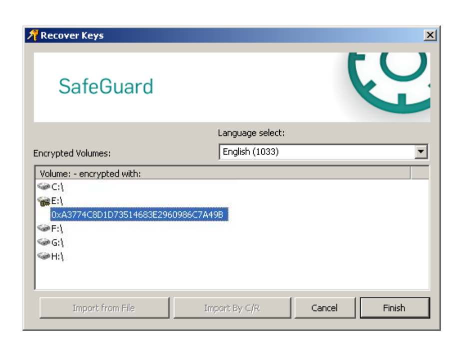
1. Wählen Sie im Windows PE Dateimanager das Laufwerk aus, auf dem der virtuelle Client gespeichert ist. Die Datei recoverytoken.tok wird auf der rechten Seite angezeigt.
2. Wählen Sie die Datei recoverytoken.tok aus und ziehen Sie sie auf das Laufwerk, auf dem sich das KeyRecovery Tool befindet. Legen Sie die Datei hier im Verzeichnis Toos\SGN-Tools ab.



29.2.6.4 Starten einer Challenge im KeyRecovery Tool

1. Klicken Sie unten im Bereich **Quick Launch** des Windows PE Dateimanagers auf das KeyRecovery-Symbol, um das KeyRecovery Tool zu öffnen. Das Key Recovery Tool zeigt die Schlüssel-ID verschlüsselter Laufwerke.

   Das Tool startet und zeigt eine Liste aller Volumes mit den jeweiligen Verschlüsselungsinformationen (Schlüssel-ID).



2. Wählen Sie das Volume, das Sie entschlüsseln möchten und klicken Sie auf **Import mit C/R**, um den Challenge-Code zu erzeugen.

   Die Datei mit dem virtuellen Client wird als Referenz in der SafeGuard Enterprise Datenbank verwendet und in der Challenge angegeben. Der Challenge-Code wird erzeugt und angezeigt.

3. Übermitteln Sie den Namen des virtuellen Clients und den Challenge-Code an den Helpdesk, z. B. über Telefon oder eine Textmitteilung. Hierzu steht eine Buchstabierhilfe zur Verfügung.

29.2.6.5 Bestätigen des virtuellen Client

Voraussetzung: Der virtuelle Client muss im SafeGuard Management Center unter **Virtuelle Clients** angelegt worden sein und er muss in der Datenbank zur Verfügung stehen.

1. Klicken Sie im SafeGuard Management Center auf **Extras > Recovery**, um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Virtueller Client**.
3. Geben Sie den Namen des virtuellen Client ein, den Sie vom Benutzer erhalten haben. Hierzu gibt es verschiedene Möglichkeiten:

   - Geben Sie den eindeutigen Namen direkt ein.

   - Wählen Sie einen Namen, indem Sie auf **[...]** im Abschnitt **Virtueller Client** des Dialogs **Recovery-Typ** klicken. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit virtuellen Clients wird angezeigt. Wählen Sie den gewünschten virtuellen Client aus und klicken Sie auf **OK**. Der Name des virtuellen Clients wird nun auf der **Recovery-Typ** Seite unter **Virtueller Client** angezeigt.

4. Klicken Sie auf **Weiter**, um den Namen der Datei mit dem virtuellen Client zu bestätigen.

Im nächsten Schritt wählen Sie die erforderliche Recovery-Aktion aus.

29.2.6.6 Auswahl der erforderlichen Recovery-Aktion

1. Wählen Sie bei **Virtueller Client** auf der **Angeforderte Aktion** Seite eine der folgenden Optionen:
   - Wählen Sie **Schlüssel angefordert**, um einen einzelnen Schlüssel für den Zugriff auf ein verschlüsseltes Volume auf dem Computer wiederherzustellen.

     Diese Option ist sowohl für zentral verwaltete Endpoints als auch für Standalone-Endpoints verfügbar.
   - Wählen Sie **Kennwort für Schlüsseldatei** angefordert, um mehrere Schlüssel für den Zugriff auf verschlüsselte Volumes auf dem Computer wiederherzustellen. Die Schlüssel werden in einer Datei gespeichert, die mit einem Zufallskennwort verschlüsselt wird, das in der Datenbank abgelegt ist. Das Kennwort ist für jede angelegte Schlüsseldatei einzigartig. Das Kennwort wird innerhalb des Response-Codes an den Zielcomputer übertragen.

     Diese Option ist nur für zentral verwaltete Endpoints verfügbar.
2. Klicken Sie auf **Weiter**.

29.2.6.7 Auswahl des angeforderten Schlüssel (einzelner Schlüssel)

Voraussetzung:

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Management Center sowie die Recovery-Aktion **Schlüssel angefordert** ausgewählt haben.

1. Wählen Sie im Recovery-Assistenten auf der Seite **Virtueller Client** aus, ob die Aktion von einem zentral verwalteten-Endpoint oder einem Standalone-Endpoint angefordert wird.
   - Wählen Sie für zentral verwaltete Endpoints **Recovery-Schlüssel für einen SafeGuard Enterprise Managed Client**. Klicken Sie auf **[...]**. In **Schlüssel suchen** können Sie sich die Schlüssel nach Schlüssel-ID oder symbolischem Namen anzeigen lassen. Klicken Sie auf **Jetzt suchen**, wählen Sie den Schlüssel und klicken Sie auf **OK**.

     Hinweis: Eine Response kann nur für zugewiesene Schlüssel erzeugt werden. Ist ein Schlüssel inaktiv, d. h. der Schlüssel ist nicht mindestens einem Benutzer zugewiesen, ist eine Response mit einem virtuellen Client nicht möglich. In diesem Fall kann der inaktive Schlüssel zunächst einem beliebigen Benutzer zugewiesen werden. Danach kann eine Response für den Schlüssel generiert werden.
   - Wählen Sie für Standalone-Endpoints **Recovery-Schlüssel für einen Sophos SafeGuard Standalone Client**. Klicken Sie neben dieser Option auf **[...]**, um nach der entsprechenden Datei zu suchen. Zur Vereinfachung der Identifizierung tragen die Recovery-Dateien den Namen des Computers: computername.GUID.xml. Wählen Sie die Datei aus und klicken Sie auf **Öffnen**.

     Hinweis: Die Schlüssel-Recovery-Datei, die zur Wiederherstellung des Zugriffs auf den Computer erforderlich ist, muss dem Helpdesk zur Verfügung stehen, z. B. über eine Netzwerkfreigabe.
2. Klicken Sie auf **Weiter**. Die Seite für die Eingabe des Challenge-Codes wird angezeigt.

Der angeforderte Schlüssel wird mit dem Response-Code an die Benutzerumgebung übertragen.

29.2.6.8 Auswahl des angeforderten Schlüssel (mehrere Schlüssel)

Voraussetzung:

Diese Option ist nur für zentral verwaltete Endpoints verfügbar.

Sie müssen die Schlüsseldatei zuvor im SafeGuard Management Center unter **Schlüssel imd Zertifikate** angelegt haben und das Kennwort, mit dem die Datei verschlüsselt ist, muss in der Datenbank gespeichert sein.

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Management Center sowie die Recovery-Aktion **Kennwort für Schlüsseldatei angefordert** ausgewählt haben.

1. Um eine Schlüsseldatei auszuwählen, klicken Sie auf die **[...]** Schaltfläche neben dieser Option. Klicken Sie in **Schlüsseldatei** auf **Jetzt suchen**. Wählen Sie die Schlüsseldatei aus und klicken Sie auf **OK**.
2. Klicken Sie zur Bestätigung auf **Weiter**.

Die Seite für die Eingabe des Challenge-Codes wird angezeigt.

29.2.6.9 Eingabe des Challenge-Codes und Erzeugen des Response-Codes

Voraussetzung:

Sie müssen den erforderlichen virtuellen Client im Recovery-Assistenten des SafeGuard Management Center sowie die erforderliche Recovery-Aktion ausgewählt haben.

1. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

   Wenn der Challenge-Code korrekt eingegeben wurde, wird der Response-Code erzeugt. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültige Challenge** angezeigt.

2. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Wenn Sie **Schlüssel angefordert** als Recovery-Aktion ausgewählt haben, wird der angeforderte Schlüssel im Response-Code an die Benutzerumgebung übertragen.

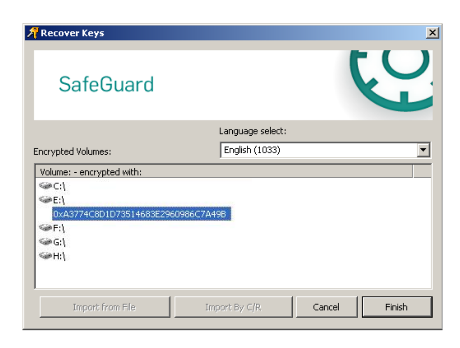
Wenn Sie **Kennwort für Schlüsseldatei angefordert** als Recovery-Aktion ausgewählte haben, wird das Kennwort für die verschlüsselte Schlüsseldatei im Response-Code übertragen. Die Schlüsseldatei wird daraufhin gelöscht.

29.2.6.10 Eingeben des Response-Codes im KeyRecovery Tool

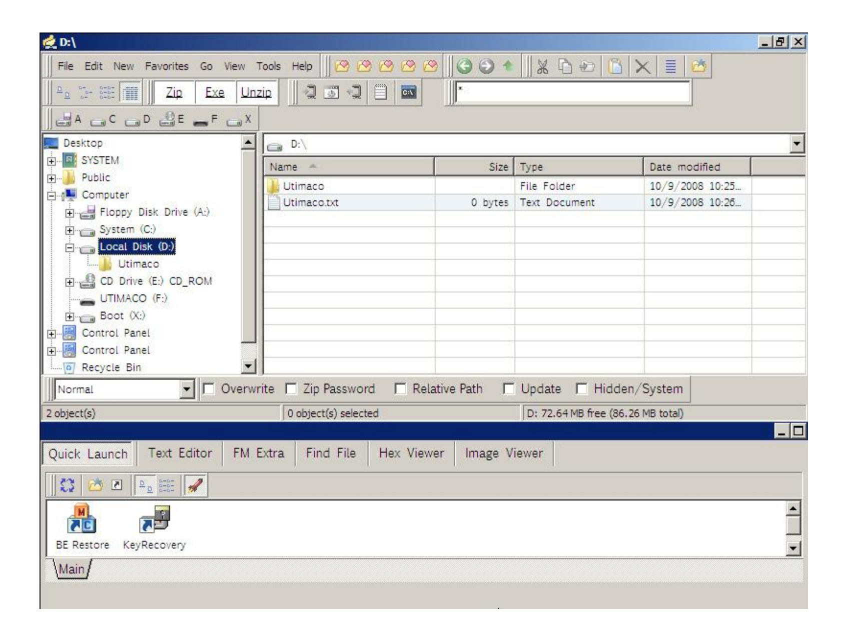
1. Geben Sie im KeyRecovery Tool auf dem Endpoint den Response-Code ein, den Sie vom Helpdesk erhalten haben.

   Mit dem Response-Code wird der erforderliche Recovery-Schlüssel übertragen.

2. Klicken Sie auf **OK**. Das für das Challenge/Response-Verfahren gewählte Laufwerk wird entschlüsselt.



3. Um sicherzustellen, dass die Entschlüsselung erfolgreich durchgeführt werden konnte, wählen Sie das entschlüsselte Laufwerk im Windows PE Dateimanager aus:



Der Inhalt des entschlüsselten Laufwerks wird nun im Dateimanager angezeigt. Das Dateisystem und die Kapazität sowie der benutzte/freie Speicherplatz werden nun in den Eigenschaften des entschlüsselten Laufwerks angegeben.

Der Zugriff auf die Daten, die auf dieser Partition gespeichert sind, ist wiederhergestellt. Nach der erfolgreichen Entschlüsselung haben Sie auf dem entsprechenden Laufwerk Lese- und Schreibzugriff für Daten. Sie können Daten vom und auf das Laufwerk kopieren.

29.2.7 Challenge/Response für Sophos SafeGuard Clients (Standalone)

SafeGuard Enterprise bietet Challenge/Response für Recovery-Vorgänge, z. B. wenn der Benutzer sein Kennwort vergessen oder es zu oft falsch eingegeben hat, auch für Standalone-Endpoints (Sophos SafeGuard Clients Standalone). Standalone-Endpoints haben nie eine Verbindung zum SafeGuard Enterprise Server, auch nicht vorübergehend. Sie werden im Standalone-Modus betrieben.

Die für Challenge/Response-Vorgänge benötigten Recovery-Informationen basieren in diesem Fall auf der Schlüssel-Recovery-Datei. Diese Schlüssel-Recovery-Datei wird auf jedem Standalone-Endpoint während der Installation der SafeGuard Enterprise Verschlüsselungssoftware erzeugt. Die Schlüssel-Recovery-Datei muss dem SafeGuard Enterprise Helpdesk zur Verfügung stehen, zum Beispiel auf einer Netzwerkfreigabe.

Um die Suche nach und die Gruppierung von Recovery-Dateien zu vereinfachen, enthalten die Dateinamen den Namen des Computers: **`computername.GUID.xml`**. Somit sind Suchvorgänge mit Asterisken (*) als Platzhalter möglich, z. B.: *.GUID.xml.

Hinweis: Wenn ein Computer umbenannt wird, wird er im Local Cache nicht automatisch entsprechend umbenannt. Im Local Cache werden alle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien gespeichert. Für die Datei-Generierung muss der neue Computername daher aus dem Local Cache entfernt werden, so dass nur der vorige Name verbleibt, auch wenn der Computer unter Windows umbenannt wird.

29.2.7.1 Recovery-Aktionen für Sophos SafeGuard Clients (standalone)

Für einen Standalone-Endpoint kann in den folgenden Situationen ein Challenge/Response-Verfahren gestartet werden:

- Der Benutzer hat das Kennwort zu oft falsch eingegeben.
- Der Benutzer hat das Kennwort vergessen.
- Ein beschädigter Local Cache muss repariert werden.

Für einen Standalone-Endpoint steht kein Benutzerschlüssel in der Datenbank zur Verfügung. Somit ist in einem Challenge/Response-Verfahren nur die Recovery-Aktion **SGN Client ohne Benutzeranmeldung booten** möglich.

Das Challenge/Response-Verfahren ermöglicht das Booten des Computers durch die SafeGuard Power-on Authentication. Der Benutzer kann sich dann an Windows anmelden.

Mögliche Recovery-Anwendungsfälle:

Der Benutzer hat das Kennwort auf SafeGuard POA-Ebene zu oft falsch eingegeben und der Computer wurde gesperrt. Der Benutzer weiß jedoch das Kennwort.

Der Computer ist gesperrt und der Benutzer wird dazu aufgefordert, ein Challenge/Response-Verfahren zu starten, um wieder Zugriff auf den Computer zu erhalten. Da der Benutzer das Kennwort noch weiß, muss es nicht zurückgesetzt werden. Das Challenge/Response-Verfahren ermöglicht das Booten des Computers durch die SafeGuard Power-on Authentication. Der Benutzer kann dann das korrekte Kennwort auf Windows-Ebene eingeben und den Computer wieder benutzen.

Der Benutzer hat das Kennwort vergessen

Hinweis: Wir empfehlen, Local Self Help einzusetzen, um ein vergessenes Kennwort wiederherzustellen. Mit Local Self Help können Benutzer sich das aktuelle Benutzerkennwort anzeigen lassen und es weiterhin zur Anmeldung verwenden. Dadurch wird ein Rücksetzen des Kennworts vermieden. Außerdem muss der Helpdesk nicht um Hilfe gebeten werden.

Wenn das Kennwort über ein Challenge/Response-Verfahren wiederhergestellt wird, muss das Kennwort zurückgesetzt werden.

1. Das Challenge/Response-Verfahren ermöglicht das Booten des Computers durch die SafeGuard Power-on Authentication.
2. Da Ihnen das Kennwort nicht bekannt ist, können der Benutzer es im Windows-Dialog nicht eingeben. Das Kennwort muss auf Windows-Ebene zurückgesetzt werden. Hierzu

sind weitere Recovery-Vorgänge außerhalb von SafeGuard Enterprise erforderlich, die über Windows-Standard-Verfahren durchgeführt werden müssen.

Hinweis: Wir empfehlen, das Kennwort vor dem Challenge/Response-Verfahren nicht zentral im Active Directory zurückzusetzen. Dadurch wird gewährleistet, dass das Kennwort zwischen Windows und SafeGuard Enterprise synchron bleibt. Stellen Sie sicher, dass der Windows-Helpdesk entsprechend informiert ist.

Wir empfehlen, die folgenden Methoden für das Zurücksetzen des Kennworts auf Windows-Ebene:

- Über ein Service-Benutzerkonto oder ein Administratorkonto mit den erforderlichen Windows-Rechten auf dem Endpoint
- Über eine Windows-Kennwortrücksetz-Diskette auf dem Endpoint

  Als Helpdesk-Beauftragter können Sie den Benutzer darüber informieren, welche Methode benutzt werden soll, und ihm die zusätzlichen Windows-Anmeldeinformationen oder die erforderliche Diskette zur Verfügung stellen.

3. Der Benutzer gibt das neue Kennwort ein, dass der Helpdesk auf Windows-Ebene zurückgesetzt hat. Unmittelbar muss der Benutzer das Kennwort in ein nur ihm bekanntes Kennwort ändern. Basierend auf dem neu gewählten Windows-Kennwort wird ein neues Benutzerzertifikat erzeugt. Dies ermöglicht es dem Benutzer, sich mit dem neuen Kennwort wieder an seinem Computer und an der SafeGuard Power-on Authentication anzumelden.

   Hinweis: Schlüssel für SafeGuard Data Exchange: Wenn ein Kennwort zurückgesetzt und ein neues Zertifikat erstellt wird, können die zuvor für SafeGuard Data Exchange erzeugten lokalen Schlüssel noch verwendet werden, wenn der Endpoint Mitglied einer Domäne ist. Wenn der Endpoint Mitglied einer Arbeitsgruppe ist, muss dem Benutzer die SafeGuard Data Exchange Passphrase bekannt sein, damit diese lokalen Schlüssel reaktiviert werden können.

Der Local Cache muss repariert werden.

Im Local Cache werden alle Schlüssel, Richtlinien, Benutzerzertifikate und Audit-Dateien gespeichert. Standardmäßig ist Recovery für die Anmeldung bei einem beschädigten Local Cache deaktiviert, d. h. der Local Cache wird automatisch aus seiner Sicherungskopie wiederhergestellt. In diesem Fall ist für das Reparieren des Local Cache kein Challenge/Response-Verfahren erforderlich. Soll der Local Cache jedoch explizit mit einem Challenge/Response-Verfahren repariert werden, so lässt sich Recovery für die Anmeldung über eine Richtlinie aktivieren. In diesem Fall wird der Benutzer bei einem beschädigten Local Cache automatisch dazu aufgefordert, ein Challenge/Response-Verfahren zu starten.

29.2.7.2 Erzeugen einer Response für Standalone-Endpoints mit der Schlüssel-Recovery-Datei

Hinweis: Die Schlüssel-Recovery-Datei, die während der Installation der SafeGuard Enterprise Verschlüsselungssoftware generiert wurde, muss an einem Speicherort abgelegt sein, auf den der Helpdesk-Beauftragte Zugriff hat. Darüber hinaus muss der Name der Datei bekannt sein.

1. Wählen Sie in der Menüleiste des SafeGuard Management Center **Extras > Recovery**, um den Recovery-Assistenten zu öffnen.
2. Wählen Sie unter **Recovery-Typ** die Option **Sophos SafeGuard Client (Standalone)**.
3. Suchen Sie nach der Schlüssel-Recovery-Datei, indem Sie auf die **[...]** Schaltfläche neben dem Feld **Schlüssel-Recovery-Datei** klicken. Zur Vereinfachung der Identifizierung tragen die Recovery-Dateien den Namen des Computers: computername.GUID.xml.

4. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**. Der Challenge-Code wird geprüft.

   Wenn der Challenge-Code korrekt eingegeben wurde, werden die vom Endpoint-Computer angeforderte Recovery-Aktion sowie die möglichen Recovery-Aktionen angezeigt. Wenn der Code nicht korrekt eingegeben wurde, wird unterhalb des Blocks, der den Fehler enthält, der Text **Ungültige Challenge** angezeigt.

5. Wählen Sie die vom Benutzer durchzuführende Aktion aus und klicken Sie auf **Weiter**.
6. Es wird ein Response-Code erzeugt. Teilen Sie den Response-Code dem Benutzer mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben, die angeforderte Aktion ausführen und dann wieder mit dem Computer arbeiten.

29.3 Recovery für BitLocker

Abhängig vom System bietet SafeGuard Enterprise ein Challenge/Response-Verfahren für die Recovery oder die Möglichkeit, beim Helpdesk den Recovery-Schlüssel zu beschaffen. Informationen darüber, welche Voraussetzungen für SafeGuard Enterprise Challenge/Response erfüllt sein müssen, finden Sie unter Voraussetzungen für die Verwaltung von BitLocker auf Endpoints (Seite 172).

29.3.1 Response für mit BitLocker verschlüsselte SafeGuard Enterprise Clients - UEFI Endpoints

Für UEFI Endpoints, die bestimmte Voraussetzungen erfüllen, bietet SafeGuard Enterprise ein Challenge/Response-Verfahren zum Recovery. Auf UEFI Endpoints, die die Voraussetzungen nicht erfüllen, wird automatisch SafeGuard BitLocker ohne Challenge/Response installiert. Informationen über die Wiederherstellung dieser Endpoints finden Sie unter Recovery-Schlüssel für mit BitLocker verschlüsselte SafeGuard Enterprise Clients - BIOS-Endpoints (Seite 255).

1. Wählen Sie auf der **Recovery-Typ** Seite die Option **SafeGuard Enterprise Client (Managed)**.
2. Wählen Sie unter **Domäne** die gewünschte Domäne aus der Liste.
3. Geben Sie unter **Computer** den gewünschten Computernamen ein oder wählen Sie ihn aus. Hierzu gibt es mehrere Möglichkeiten:
   - Um einen Namen auszuwählen, klicken Sie auf **[...]**. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird auf der Seite **Recovery-Typ** angezeigt.
   - Geben Sie den Kurznamen des Computers direkt in das Feld ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     `CN=Desktop1,OU=Development,OU=Headquarter,DC=Sophos,DC=edu`

4. Klicken Sie auf **Weiter**.
5. Wählen Sie das Volume, auf das zugegriffen werden soll, aus der Liste und klicken Sie auf **Weiter**.

6. Klicken Sie auf **Weiter**.

   Eine Seite für die Eingabe des Challenge-Codes wird angezeigt.

7. Geben Sie den vom Benutzer erhaltenen Challenge-Code ein und klicken Sie auf **Weiter**.
8. Es wird ein Response-Code erzeugt. Teilen Sie dem Benutzer den Response-Code mit. Hierzu steht eine Buchstabierhilfe zur Verfügung. Sie können den Response-Code auch in die Zwischenablage kopieren.

Der Benutzer kann den Response-Code eingeben und wieder auf den Endpoint zugreifen.

29.3.2 Recovery-Schlüssel für mit BitLocker verschlüsselte SafeGuard Enterprise Clients - BIOS Endpoints

Bei mit BitLocker verschlüsselten Computern lässt sich ein Volume, auf das nicht mehr zugegriffen werden kann, wiederherstellen.

1. Wählen Sie auf der **Recovery-Typ** Seite die Option **SafeGuard Enterprise Client (Managed)**.
2. Wählen Sie unter **Domäne** die gewünschte Domäne aus der Liste.
3. Geben Sie unter **Computer** den gewünschten Computernamen ein oder wählen Sie ihn aus. Hierzu gibt es mehrere Möglichkeiten:
   - Um einen Namen auszuwählen, klicken Sie auf **[...]**. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird im Fenster **Recovery-Typ** unter **Domäne** angezeigt.
   - Geben Sie den Kurznamen des Computers direkt in das Feld ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     `CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu`

4. Klicken Sie auf **Weiter**.
5. Wählen Sie das Volume, auf das zugegriffen werden soll, aus der Liste und klicken Sie auf **Weiter**.
6. Der Recovery-Assistent zeigt den 48-stelligen Recovery-Schlüssel an.
7. Teilen Sie dem Benutzer diesen Schlüssel mit.

Der Benutzer kann den Schlüssel eingeben, um den Zugriff auf das mit BitLocker verschlüsselte Volume auf dem Endpoint wiederherzustellen.

29.4 Recovery-Schlüssel für Mac-Endpoints

Der Zugriff auf mit FileVault 2 verschlüsselte SafeGuard Enterprise Clients kann mit folgenden Schritten wiederhergestellt werden:

1. Wählen Sie auf der **Recovery-Typ** Seite die Option **SafeGuard Enterprise Client (Managed)**.
2. Wählen Sie unter **Domäne** die gewünschte Domäne aus der Liste.

3. Geben Sie unter **Computer** den gewünschten Computernamen ein oder wählen Sie ihn aus. Hierzu gibt es mehrere Möglichkeiten:
   - Um einen Namen auszuwählen, klicken Sie auf **[...]**. Klicken Sie anschließend auf **Jetzt suchen**. Eine Liste mit Computern wird angezeigt. Wählen Sie den gewünschten Computer aus und klicken Sie auf **OK**. Der Computername wird im Fenster **Recovery-Typ** unter **Domäne** angezeigt.
   - Geben Sie den Kurznamen des Computers direkt in das Feld ein. Wenn Sie auf **Weiter** klicken, wird der Name in der Datenbank gesucht. Der gefundene Computername wird als Distinguished Name angezeigt.
   - Geben Sie den Computernamen direkt als Distinguished Name ein, zum Beispiel:

     `CN=Desktop1,OU=Development,OU=Headquarter,DC=Utimaco,DC=edu`
4. Klicken Sie auf **Weiter**.
5. Der Recovery-Assistent zeigt den 24-stelligen Recovery-Schlüssel an.
6. Teilen Sie dem Benutzer diesen Schlüssel mit.

Der Benutzer kann den Recovery-Schlüssel eingeben, um sich am Mac-Endpoint anzumelden und das Kennwort zurückzusetzen.

29.5 System-Recovery für die Sophos SafeGuard Festplattenverschlüsselung

SafeGuard Enterprise verschlüsselt Dateien und Laufwerke transparent. Darüber hinaus können auch Bootlaufwerke verschlüsselt werden, so dass Entschlüsselungsfunktionalitäten wie Code, Verschlüsselungsalgorithmen und Verschlüsselungsschlüssel sehr früh in der Bootphase verfügbar sein müssen. Folglich kann auf verschlüsselte Informationen nicht zugegriffen werden, wenn entscheidende SafeGuard Enterprise Module nicht verfügbar sind oder nicht funktionieren.

Die folgenden Abschnitte beschreiben mögliche Probleme und Recovery-Verfahren.

29.5.1 Daten-Recovery durch Booten von einem externen Medium

Dieser Recovery-Typ kann angewendet werden, wenn sich der Benutzer nicht mehr auf das verschlüsselte Volume zugreifen kann. In diesem Fall kann der Zugriff auf die verschlüsselten Daten durch Booten des Computers über eine für SafeGuard Enterprise angepasste Windows PE Recovery Disk wiederhergestellt werden.

Voraussetzungen:

- Der Benutzer, der vom externen Medium bootet, muss dazu berechtigt sein. Das muss im BIOS des Computers so konfiguriert sein.
- Der Computer muss das Booten von anderen Medien außer von der fest eingebauten Festplatte unterstützen.

So erhalten Sie wieder Zugriff auf die verschlüsselten Daten auf dem Computer:

1. Fordern Sie beim technischen Support von Sophos die SafeGuard Enterprise Windows PE Disk an.

   Für den Helpdesk steht die Windows PE Recovery Disk mit den aktuellen SafeGuard Enterprise Filter-Treibern auf der Sophos Support-Website zum Download zur Verfügung. Weitere Informationen finden Sie unter http://www.sophos.com/de-de/support/knowledgebase/108805.aspx.

2. Legen Sie die Windows PE Recovery Disk ein.
3. Starten Sie den Computer von der Recovery Disk und führen Sie ein Challenge/Response mit einem virtuellen Client durch. Weitere Informationen finden Sie unter Challenge/Response mit virtuellen Clients (Seite 245).

Der Zugriff auf die Daten, die auf dieser Partition gespeichert sind, ist wiederhergestellt.

Hinweis: Je nach verwendetem BIOS funktioniert das Booten von der Disk u. U. nicht.

29.5.2 Beschädigter MBR

Zur Problembehebung im Fall eines beschädigten MBR bietet SafeGuard Enterprise das Tool **`BE_Restore.exe`**.

Eine detaillierte Beschreibung zur Wiederherstellung eines beschädigten MBR finden Sie in der *SafeGuard Enterprise Tools-Anleitung*.

29.5.3 Beschädigter Kernel-Bootcode

Es kann auf eine Festplatte mit einem beschädigten Kernel-Bootcode zugegriffen werden. Denn Schlüssel werden getrennt vom Kernel in der so genannten KSA (Key Storage Area) gespeichert. Durch die Trennung von Kernel und Schlüsseln können solche Laufwerke angeschlossen an einen anderen Computer entschlüsselt werden.

Dazu benötigt der Benutzer, der sich an dem anderen Computer anmeldet, einen Schlüssel der KSA der nicht bootbaren Partition in seinem Schlüsselring.

Im schlimmsten Fall ist die Partition nur mit dem Boot_Key des anderen Computers verschlüsselt. In diesem Fall muss der Haupt-Sicherheitsbeauftragte oder der Recovery-Beauftragte dem Benutzer diesen Boot_Key zuweisen.

Weitere Informationen finden Sie unter "Slaven" einer Festplatte (Seite 259).

29.5.4 Volumes

SafeGuard Enterprise bietet die volume-basierende Verschlüsselung. Dies beinhaltet die Speicherung von Verschlüsselungsinformationen bestehend aus Bootsektor, primärer bzw. Backup-KSA und Originalbootsektor auf jedem Laufwerk selbst.

Wenn eine der folgenden Bedingungen zutrifft, besteht auf das jeweilige Volume kein Zugriff mehr:

- Beide Key Storage Areas (KSA) sind zur gleichen Zeit beschädigt.
- Der Original-MBR ist beschädigt.

29.5.4.1 Bootsektor

Der Bootsektor eines Volumes wird bei der Verschlüsselung gegen den SafeGuard Enterprise Bootsektor ausgetauscht.

Der SafeGuard Enterprise Bootsektor enthält Informationen über

- den Ort der primären und Backup-KSA in Clustern und Sektoren bezogen auf den Start der Partition
- die Größe der KSA

Auch wenn der SafeGuard Enterprise Bootsektor zerstört ist, ist kein Zugriff auf verschlüsselte Volumes möglich.

Das Tool **`BE_Restore`** kann den zerstörten Bootsektor wiederherstellen. Weitere Informationen hierzu finden Sie in der *SafeGuard Enterprise Tools-Anleitung*.

29.5.4.2 Originaler Bootsektor

Beide KSAs enthalten den originalen Bootsektor. Das ist jener, der ausgeführt wird, nachdem der DEK (Data Encryption Key) entschlüsselt wurde und der Algorithmus und der Schlüssel in den BE Filtertreiber geladen wurden.

Ist dieser Bootsektor defekt, kann Windows nicht auf das Volume zugreifen. Normalerweise wird die bekannte Fehlermeldung „Gerät ist nicht formatiert. Möchten Sie es jetzt formatieren? Ja/Nein“ angezeigt.

SafeGuard Enterprise wird den DEK für dieses Volume dennoch laden. Jedes Tool, das den Bootsektor reparieren kann, soll dennoch laufen - vorausgesetzt, es passiert den SafeGuard Enterprise Upper Volume Filter.

29.5.5 Windows Bootprobleme

SafeGuard Enterprise ist mit seinem kryptographischen Konzept der volume-spezifischen Schlüssel (Bootsektor, Key Storage Area KSA) sehr flexibel.

Sie können ein beschädigtes System durch Booten eines Wiederherstellungsmediums von der SafeGuard Power-on Authentication aus (Windows PE mit dem SafeGuard Enterprise Verschlüsselungs-Subsystem installiert) retten. Diese Medien haben einen transparenten Ver-/Entschlüsselungszugriff auf mit SafeGuard Enterprise verschlüsselte Volumes. Der Grund für das nicht bootbare System kann von dort aus beseitigt werden.

29.5.5.1 Verschlüsselungs-Subsystem

Verschlüsselungs-Subsysteme sind z. B. BEFLT.sys Systeme. Führen Sie das unter Windows Bootprobleme beschriebene Verfahren aus und reparieren Sie das System.

29.5.6 Setup WinPE für SafeGuard Enterprise

Um Zugriff auf verschlüsselte Laufwerke mit dem BOOTKEY eines Computers innerhalb einer WinPE Umgebung zu erhalten, stellt SafeGuard Enterprise WinPE mit notwendigen SafeGuard Enterprise Funktionsmodulen wie Treibern zur Verfügung. Um SetupWinPE zu starten, geben Sie folgenden Befehl ein:

```
SetupWinPE -pe2 <WinPE Image-Datei>
```

`WinPE Image-Datei` ist dabei die vollständige Pfadangabe des I386 Verzeichnisses für eine WinPE-CD.

SetupWinPE führt alle erforderlichen Änderungen durch.

Hinweis: Über eine derartige WinPE-Umgebung kann nur auf verschlüsselte Laufwerke zugegriffen werden, die mit dem BOOTKEY verschlüsselt sind. Auf Laufwerke, die mit einem Benutzerschlüssel verschlüsselt sind, kann nicht zugegriffen werden, da die Schlüssel in dieser Umgebung nicht verfügbar sind.

29.5.7 „Slaven“ einer Festplatte

SafeGuard Enterprise erlaubt das Slaven von verschlüsselten Volumes oder Festplatten. Es gestattet dem Endbenutzer, dem Windows-Administrator, dem SafeGuard Enterprise Sicherheitsbeauftragten trotz sektorbasierter Verschlüsselung neue Volumes oder Festplatten anzuschließen oder zu entfernen.

Die Key Storage Area (KSA) eines Volumes enthält selbst alle notwendigen Informationen:

- Den zufallsgenerierten DEK (Data Encryption Key)
- Eine Identifikation für den Verschlüsselungsalgorithmus, mit dem das Volume verschlüsselt ist.
- Die Liste von GUIDs der KEKs (Key Encryption Keys), die den DEK verschlüsseln und entschlüsseln können.
- Das Volume selbst enthält seine Größe.

Auf ein mit SafeGuard Enterprise verschlüsseltes Volume kann von allen SafeGuard Enterprise Endpoints zugegriffen werden, vorausgesetzt der Benutzer oder der Computer besitzt einen KEK des KSA des Volumes im Schlüsselring.

Benutzer oder Computer müssen den durch den KEK verschlüsselten DEK entschlüsseln können.

Auf ein Volume, das mit einem verteilbaren KEK, wie einem OU-, Gruppen- oder Domänenschlüssel verschlüsselt ist, kann von vielen Benutzern und Computern zugegriffen werden, da viele Benutzer/Computer einer Domäne diesen Schlüssel in ihrem Schlüsselring haben.

Jedoch kann auf ein Volume, das nur mit dem individuellen Bootschlüssel (“Boot_machinename”) des durch SafeGuard Enterprise geschützten Endpoint verschlüsselt wird, nur von diesem Computer selbst zugegriffen werden.

Soll ein Volume nicht in seinem originalen Computer booten, kann es in einem anderen durch SafeGuard Enterprise geschützten Endpoint „geslaved“ werden. Dann kann aber auf den korrekten Bootschlüssel nicht zugegriffen werden. Der Zugriff darauf muss möglich gemacht werden.

Immer wenn der Benutzer versucht, von einem anderen Computer auf das Volume zuzugreifen, ist dies möglich, weil jetzt erneut Übereinstimmung zwischen den KEKs im KSA und den Schlüsselringen der anderen Benutzer oder Computer besteht.

29.5.7.1 Beispiel

Alice besitzt ihren individuellen Benutzerschlüssel. Immer, wenn sie sich an ihrem anderen Computer anmeldet (“Laptop_Alice”), hat sie keinen Zugriff auf das Volume, das mit dem Bootschlüssel des Computers “SGNCLT” verschlüsselt ist.

Der durch SafeGuard Enterprise geschützte Endpoint “SGMCLT” besitzt nur seinen eigenen Bootschlüssel BOOT_SGMCLT.

Der Sicherheitsbeauftragte teilt Alice den Bootschlüssel “BOOT_SGNCLT” auf folgende Weise zu:

1. Auswahl des Benutzers Alice
2. Klick auf das „Fernglas“-Symbol in der SafeGuard Enterprise Symbolleiste. Das startet den Suchdialog, in dem auch Bootschlüssel angezeigt werden können.
3. Auswahl des Schlüssels “BOOT_SGMCLT”.

Jetzt verfügt Alice über zwei Schlüssel – „User_Alice“ und „BOOT_SGMCLT“. Das kann unter **Schlüssel und Zertifikate** nachgeprüft werden.

Der Schlüssel “BOOT_SGMCLT” ist zweimal zugewiesen – zum Computer SGMCLT und zum Benutzer Alice.

Alice ist es nun möglich, auf das verschlüsselte Volume von jedem anderen SafeGuard Enterprise Client zuzugreifen, auf dem sie sich anmelden kann.

Dann kann sie auf einfache Weise Tools, wie den Windows Explorer oder regedit.exe, verwenden, um die Ursache des Bootproblems zu beseitigen.

Wenn im schlimmsten Fall das Problem nicht gelöst werden kann, kann sie Daten auf ein anderes Laufwerk sichern, das Volume neu formatieren oder es ganz neu aufsetzen.

30 Wiederherstellen einer beschädigten SafeGuard Enterprise Installation

Eine beschädigte SafeGuard Management Center Installation kann auf einfache Art und Weise wiederhergestellt werden, wenn die Datenbank noch intakt ist. In diesem Fall müssen Sie nur das SafeGuard Management Center neu installieren und die vorhandene Datenbank sowie das gesicherte Sicherheitsbeauftragten-Zertifikat verwenden.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

So stellen Sie eine beschädigte SafeGuard Management Center Installation wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der Konfigurationsassistent wird automatisch geöffnet.
2. Wählen Sie unter **Datenbankverbindung** den relevanten Datenbankserver und konfigurieren Sie, falls erforderlich, die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Aktivieren Sie unter **Datenbankeinstellungen** die Option **Folgende bestehende Datenbank verwenden** und wählen Sie die Datenbank aus der Liste aus.
4. Führen Sie unter **Daten des Sicherheitsbeauftragten** einen der folgenden Schritte aus:
   - Wenn die gesicherte Zertifikatsdatei auf dem Computer gefunden wird, wird sie angezeigt. Geben Sie das Kennwort ein, das Sie zur Anmeldung an das SafeGuard Management Center benutzen.
   - Wird die gesicherte Zertifikatsdatei nicht auf dem Computer gefunden, wählen Sie **Importieren**. Suchen Sie nach der gesicherten Zertifikatsdatei und klicken Sie auf **Öffnen**. Geben Sie das Kennwort für die Zertifikatsdatei ein. Klicken Sie auf **Ja**. Geben Sie ein Kennwort für die Anmeldung am SafeGuard Management Center ein und bestätigen Sie es.
5. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um die Konfiguration des SafeGuard Management Center abzuschließen.

Die SafeGuard Management Center Installation ist wiederhergestellt.

31 Wiederherstellen einer beschädigten Datenbankkonfiguration

Sie können eine beschädigte Datenbankkonfiguration wiederherstellen, indem Sie das SafeGuard Management Center neu installieren und basierend auf den gesicherten Zertifikatsdateien eine neue Instanz der Datenbank erstellen. Dadurch wird sichergestellt, dass alle vorhandenen SafeGuard Enterprise Endpoints Richtlinien von der neuen Installation annehmen.

- Das Unternehmenszertifikat und das Haupt-Sicherheitsbeauftragten-Zertifikat der betreffenden Datenbankkonfiguration müssen als .p12 Dateien exportiert worden sein. Die Dateien müssen vorhanden und gültig sein.
- Die Kennwörter für die beiden .p12 Dateien sowie für den Zertifikatsspeicher müssen Ihnen bekannt sein.

Hinweis: Diese Art der Wiederherstellung ist nur dann zu empfehlen, wenn keine gültige Sicherungskopie der Datenbank verfügbar ist. Alle Computer, die mit einem Backend verbunden sind, das auf diese Weise wiederhergestellt wurde, verlieren ihre Benutzer-Computer Zuordnung. Dies führt zu einer vorübergehenden Deaktivierung der SafeGuard Power-on Authentication. Challenge/Response-Mechanismen stehen erst dann wieder zur Verfügung, wenn der entsprechende Endpoint seine Schlüsselinformationen wieder erfolgreich übertragen hat.

So stellen Sie eine beschädigte Datenbankkonfiguration wieder her:

1. Installieren Sie das SafeGuard Management Center Installationspaket neu. Öffnen Sie das SafeGuard Management Center. Der **Konfigurationsassistent** wird automatisch geöffnet.
2. Wählen Sie unter **Datenbank-Verbindung** die Option **Neue Datenbank erstellen**. Konfigurieren Sie unter **Datenbankeinstellungen** die Verbindung zur Datenbank. Klicken Sie auf **Weiter**.
3. Wählen Sie unter **Daten des Sicherheitsbeauftragten** den relevanten Haupt-Sicherheitsbeauftragten und klicken Sie auf **Importieren**.
4. Suchen Sie unter **Importieren des Zertifikats** die gesicherte Zertifikatsdatei. Geben Sie unter **Schlüsseldatei** das für diese Datei festgelegte Kennwort ein und bestätigen Sie es. Klicken Sie auf **OK**.
5. Das Zertifikat des Haupt-Sicherheitsbeauftragten wird importiert. Klicken Sie auf **Weiter**.
6. Aktivieren Sie unter **Unternehmenszertifikat** die Option **Über vorhandenes Unternehmenszertifikat wiederherstellen**. Klicken Sie auf **Importieren**, um die gesicherte Zertifikatsdatei auszuwählen, die das gültige Unternehmenszertifikat enthält. Sie werden aufgefordert, das für den Zertifikatsspeicher definierte Kennwort einzugeben. Geben Sie das Kennwort ein und klicken Sie auf **OK**. Klicken Sie im Willkommen-Fenster auf **Weiter**.

   Das Unternehmenszertifikat wird importiert.
7. Klicken Sie auf **Weiter**, dann auf **Beenden**.

Die Datenbankkonfiguration ist wiederhergestellt.

32 Bestands- und Statusinformationen

SafeGuard Enterprise liest eine Fülle von Bestands- und Statusinformationen von den Endpoints aus. Diese Informationen zeigen den aktuellen globalen Zustand der einzelnen Computer. Im SafeGuard Management Center werden die Informationen im Bereich **Benutzer & Computer** in der Registerkarte **Bestand** dargestellt.

Als Sicherheitsbeauftragter können Sie Bestands- und Statusinformationen einsehen, exportieren und drucken. So können Sie z. B. Compliance-Berichte erstellen, die die Verschlüsselung von Endpoints nachweisen. Umfassende Sortier- und Filterfunktionen unterstützen Sie bei der Auswahl der relevanten Informationen.

Der **Bestand** liefert u. a. folgende Informationen zu den einzelnen Maschinen:

- Erhaltene Richtlinien
- Letzter Server-Kontakt
- Verschlüsselungsstatus aller Medien
- POA-Status und Typ
- Installierte SafeGuard Enterprise Module
- WOL-Status
- Benutzerinformationen

32.1 Mac-Endpoints im Bestand

Der **Bestand** liefert Statusdaten für im SafeGuard Management Center verwaltete Macs. Weitere Informationen finden Sie unter Bestands- und Statusinformationen für Macs (Seite 293)

32.2 Einsehen von Bestandsinformationen

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf **Benutzer & Computer**.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf den jeweiligen Container (Domäne, Arbeitsgruppe oder Computer).
3. Wechseln Sie im Aktionsbereich auf der rechten Seite in die Registerkarte **Bestand**.
4. Wählen Sie im Bereich **Filter** die gewünschten Filter für die Bestandsanzeige (siehe Filtern von Bestandsinformationen (Seite 264)).

   Hinweis: Wenn Sie einen einzelnen Computer wählen, stehen die Bestandsinformationen direkt nach dem Wechsel in die Registerkarte **Bestand** zur Verfügung. Der Bereich **Filter** ist hier nicht verfügbar.

5. Klicken Sie im Bereich **Filter** auf das Lupensymbol.

Die Bestands- und Statusinformationen werden in einer Übersichtstabelle für alle Maschinen des ausgewählten Containers angezeigt. Darüber hinaus stehen für die einzelnen Maschinen die Registerkarten **Laufwerke**, **Benutzer** und **Merkmale** zur Verfügung.

Durch Klicken auf die einzelnen Spalten-Header lassen sich die Bestands- und Statusinformationen nach den jeweiligen Spalteninformationen sortieren. Darüber hinaus steht über das Kontextmenü der einzelnen Spalten eine Reihe von Funktionen für die Sortierung, Gruppierung und Anpassung der angezeigten Anzeige zur Verfügung. Je nach Ihren Zugriffsrechten werden die Informationen im Bestand in unterschiedlichen Farben angezeigt:

- Informationen für Objekte, für die Sie das Recht **Voller Zugriff** haben, werden schwarz angezeigt.
- Informationen für Objekte, für die Sie das Recht **Schreibgeschützt** haben, werden blau angezeigt.
- Informationen für Objekte, für die Sie keine Zugriffsrechte haben, werden grau angezeigt.

32.3 Anzeigen ausgeblendeter Spalten

Einige Spalten sind in der Bestandsanzeige standardmäßig ausgeblendet.

1. Klicken Sie mit der rechten Maustaste in die Spaltenkopfzeilenleiste der Bestandsanzeige.
2. Wählen Sie aus dem Kontextmenü den Befehl **Laufende Spaltenanpassung**.

   Das Fenster **Anpassung** mit den ausgeblendeten Spalten wird angezeigt.

3. Ziehen Sie die gewünschte Spalte aus dem Fenster **Anpassung** in die Spaltenkopfzeilenleiste.

Die Spalte wird in der Bestandsanzeige angezeigt. Um die Spalte wieder auszublenden, ziehen Sie sie zurück in das Fenster **Anpassung**.

32.4 Filtern von Bestandsinformationen

Für die Übersicht der Bestandsinformationen für OUs lassen sich Filter definieren, um die Darstellung nach bestimmten Kriterien einzuschränken.

Im **Filter**-Bereich der Registerkarte **Bestand** stehen folgende Felder für die Definition von Filtern zur Verfügung:

Feld	Beschreibung
Computername	Um die Bestand- und Statusinformationen für bestimmte Computer anzeigen zu lassen, geben Sie in diesem Feld den Computernamen an.
Einschließlich Sub-Container	Aktivieren Sie dieses Feld, um Sub-Container in die Anzeige mit einzubeziehen.
Letzte Änderung anzeigen	Legen Sie in diesem Feld die Anzahl der anzuzeigenden letzten Änderungen festlegen.

Darüber hinaus können Sie mit dem Filter-Editor benutzerdefinierte Filter erstellen. Der Filter-Editor lässt sich über das Kontextmenü der einzelnen Berichtsspalten aufrufen. Im Fenster **Filterdefinition** können Sie eigene Filter definieren und auf die jeweilige Spalte anwenden.

32.5 Aktualisieren von Bestandsinformationen

Die Endpoints übertragen die jeweils aktuellen Bestandsinformationen, wenn sich die Informationen geändert haben.

Über den Befehl **Aktualisierung anfordern** können Sie manuell eine Aktualisierung der Bestandsinformationen anfordern. Dieser Befehl steht für einen einzelnen oder alle Computer eines Knotens über das Kontextmenü sowie über das Menü **Aktionen** in der SafeGuard Management Center Menüleiste zur Verfügung. Darüber hinaus lässt sich der Befehl über das Kontextmenü der Listeneinträge auswählen.

Wenn Sie diesen Befehl auswählen oder auf das Symbol **Aktualisierung anfordern** in der Symbolleiste klicken, übertragen die jeweiligen Endpoint-Computer ihre aktuellen Bestandsinformationen.

Wie auch in anderen Bereichen des SafeGuard Management Center, können Sie die Anzeige mit dem Befehl **Aktualisieren** aktualisieren. Sie können diesen Befehl aus dem Kontextmenü für einzelne Computer oder alle Computer in einem Knoten auswählen. Der Befehl steht außerdem im **Ansicht** Menü in der Menüleiste zur Verfügung. Zur Aktualisierung der Ansicht können Sie auch das Doppelpfeilsymbol **Aktualisieren** in der Symbolleiste wählen.

32.6 Überblick

Die einzelnen Spalten der Übersicht zeigen folgende Informationen.

Hinweis: Einige Spalten sind standardmäßig ausgeblendet. Sie können diese in der Anzeige einblenden. Weitere Informationen finden Sie unter Anzeigen ausgeblendeter Spalten (Seite 264).

Spalte	Erklärung
Computername	Zeigt den Namen des Computers.
Domäne	Zeigt den Domänennamen des Computers.
Domäne Prä-2000	Zeigt den Domänennamen des Computers vor Windows 2000.
Benutzername (Besitzer)	Zeigt den Benutzernamen des Besitzers des Computers, falls verfügbar.
Vorname	Zeigt den Vornamen des Besitzers, falls verfügbar.
Nachname	Zeigt den Nachnamen des Besitzers, falls verfügbar.
E-Mail-Adresse	Zeigt die E-Mail-Adresse des Besitzers, falls verfügbar.
Weitere registrierte Benutzer	Zeigt die Namen von weiteren registrierten Benutzern des Computers, falls verfügbar.

Spalte	Erklärung
Betriebssystem	Zeigt das Betriebssystem des Computers.
Letzter Server-Kontakt	Zeigt an, wann (Datum und Uhrzeit) der Computer zuletzt mit dem Server kommuniziert hat.
Zuletzt erhaltene Richtlinie	Zeigt an, wann (Datum und Uhrzeit) der Computer die letzte Richtlinie erhalten hat.
Verschlüsselte Laufwerke	Zeigt die verschlüsselten Laufwerke des Computers.
Unverschlüsselte Laufwerke	Zeigt die unverschlüsselten Laufwerke des Computers.
POA Typ	Gibt an, ob der Computer ein nativer SafeGuard Enterprise Endpoint, ein BitLocker Endpoint mit Challenge/Response, ein BitLocker Endpoint mit eingebautem Recovery-Mechanismus, ein FileVault 2 Endpoint oder ein Endpoint mit einer selbst-verschlüsselnden Opal-Festplatte ist.
POA	Gibt an, ob die SafeGuard Power-on Authentication für den Computer aktiviert ist.
WOL	Gibt an, ob Wake on LAN für den Computer aktiviert ist.
Änderungsdatum	Zeigt das Datum, an dem sich die Bestandsinformationen durch Anforderung einer Bestandsaktualisierung oder Übermittlung neuer Bestandsinformationen vom Client geändert haben.
Aktualisierung angefordert	Zeigt das Datum der letzten Aktualisierungsanforderung an. Der in diesem Feld angezeigte Wert wird bei der Verarbeitung der Anforderung durch den Client wieder gelöscht.
Stamm-DSN	Zeigt den Distinguished Name des dem Computer übergeordneten Containerobjekts an. Diese Spalte wird nur dann angezeigt, wenn im **Filter**-Bereich das Feld **Einschließlich Sub-Container** aktiviert wurde.
Aktuelles Unternehmenszertifikat	Gibt an, ob der Computer das aktuelle Unternehmenszertifikat verwendet.

32.7 Registerkarte Laufwerke

Die Registerkarte **Laufwerke** zeigt Bestands- und Statusinformationen zu den Laufwerken des jeweiligen Computers.

Spalte	Erklärung
Laufwerksname	Zeigt den Laufwerksnamen an.
Label	Zeigt das Label eines Mac-Laufwerks.

Spalte	Erklärung
Typ	Zeigt den Laufwerkstyp an, z. B. **Fest**, **Wechseldatenträger** oder **CD-ROM/DVD**.
Status	Zeigt den Verschlüsselungsstatus eines Laufwerks an. **Hinweis:** Wenn SafeGuard BitLocker Verwaltung auf einem Endpoint installiert ist, kann **Nicht vorbereitet** als Verschlüsselungsstatus eines Laufwerks angezeigt werden. Das bedeutet, dass das Laufwerk momentan nicht mit BitLocker verschlüsselt werden kann, weil notwendige Vorbereitungen noch nicht durchgeführt wurden. Das trifft nur auf verwaltetete Endpoints zu, weil nicht verwaltetete Endpoints keine Bestandsinformationen melden können. Informationen zu den Voraussetzungen für die Verwaltung und Verschlüsselung von BitLocker-Laufwerken finden Sie unter Voraussetzungen für die Verwaltung von BitLocker auf Endpoints (Seite 172). Der Verschlüsselungsstatus eines nicht verwalteten Endpoints kann mit dem Kommandozeilen-Tool SGNState überprüft werden. Detaillierte Informationen hierzu finden Sie in der *SafeGuard Enterprise Tools-Anleitung.*
Algorithmus	Zeigt für verschlüsselte Laufwerke den Algorithmus, der zur Verschlüsselung benutzt wurde, an.

32.8 Registerkarte Benutzer

Die Registerkarte **Benutzer** zeigt Bestands- und Statusinformationen zu den Benutzern des Computers.

Spalte	Erklärung
Benutzername	Zeigt den Benutzernamen des Benutzers.
Distinguished Name	Zeigt den DNS-Namen für den Benutzer, zum Beispiel: CN=Administrator,CN=Users,DC=domain,DC=mycompany,DC=net
Benutzer ist Besitzer	Gibt an, ob der Benutzer als Besitzer des Computers definiert ist.
Benutzer ist gesperrt	Gibt an, ob der Benutzer gesperrt ist.
SGN Windows-Benutzer	Gibt an, ob es sich um einen SGN Windows-Benutzer handelt. Ein SGN Windows-Benutzer wird nicht zur SafeGuard POA hinzugefügt, verfügt jedoch über einen Schlüsselring, mit dem er wie ein SGN-Benutzer auf verschlüsselte Dateien zugreifen kann. Sie können die Registrierung von SGN Windows-Benutzern auf Endpoints über Richtlinien des Typs **Spezifische Computereinstellungen** aktivieren.

32.9 Registerkarte Module

Die Registerkarte **Module** liefert eine Übersicht zu allen auf dem Computer installierten SafeGuard Enterprise Modulen.

Spalte	Erklärung
Modulname	Zeigt den Namen des installierten SafeGuard Enterprise Moduls.
Version	Zeigt die Software-Version des installierten SafeGuard Enterprise Moduls.

32.10 Registerkarte Unternehmenszertifikat

Die Registerkarte **Unternehmenszertifikat** zeigt die Eigenschaften des derzeit verwendeten Unternehmenszertifikats und gibt an, ob ein neueres Unternehmenszertifikat verfügbar ist.

Spalte	Erklärung
Antragsteller	Zeigt den Distinguished Name des Antragstellers des Unternehmenszertifikats.
Seriennummer	Zeigt die Seriennummer des Unternehmenszertifikats.
Aussteller	Zeigt den Distinguished Name des Ausstellers des Unternehmenszertifikats.
Gültig ab	Zeigt das Datum und die Uhrzeit, ab das Unternehmenszertifikat gültig wird.
Gültig bis	Zeigt das Datum und die Uhrzeit, ab das Unternehmenszertifikat ungültig wird.
Ein neueres Unternehmenszertifikat ist verfügbar	Gibt an, ob ein neueres Unternehmenszertifikat als das aktuelle des Endpoints verfügbar ist.

32.11 Erstellen von Bestandsberichten

Als Sicherheitsbeauftragter können Sie Bestandsberichte in unterschiedlichen Formaten erstellen. So können Sie z. B. Compliance-Berichte erstellen, die die Verschlüsselung von Endpoints nachweisen. Sie können die Berichte drucken oder in eine Datei exportieren.

32.11.1 Drucken von Bestandsberichten

1. Klicken Sie in der SafeGuard Management Center Menüleiste auf **Datei**.
2. Sie können den Bericht sofort drucken oder zunächst eine Druckvorschau anzeigen lassen.

   Die Druckvorschau bietet eine Reihe von Funktionen, z. B. für die Bearbeitung des Seitenlayouts (Kopf- und Fußzeile usw.).

   - Um eine Druckvorschau anzuzeigen, wählen Sie **Datei > Druckvorschau**.
   - Um das Dokument sofort zu drucken, wählen Sie **Datei > Drucken**.

32.11.2 Export von Bestandsberichte in Dateien

1. Klicken Sie in der SafeGuard Management Center Menüleiste auf **Datei**.
2. Wählen Sie **Drucken > Druckvorschau**.

   Die Bestandsbericht **Druckvorschau** wird angezeigt.

   Die Druckvorschau bietet eine Reihe von Funktionen, z. B. für die Bearbeitung des Seitenlayouts (Kopf- und Fußzeile usw.).

3. Klicken Sie in der Symbolleiste des Fensters **Druckvorschau** auf die Dropdownliste des Symbols **Dokument exportieren...**.
4. Wählen Sie den gewünschten Dateityp aus der Liste.
5. Geben Sie die gewünschten Exportoptionen an und klicken Sie auf **OK**.

Der Bestandsbericht wird in eine Datei des angegebenen Dateityps exportiert.

33 Berichte

Die Aufzeichnung sicherheitsrelevanter Vorfälle ist Voraussetzung für eine gründliche Systemanalyse. Anhand der protokollierten Ereignisse können Vorgänge auf einer Arbeitsstation bzw. innerhalb eines Netzwerks exakter nachvollzogen werden. Durch die Protokollierung lassen sich zum Beispiel Schutzverletzungen unautorisierter Dritter nachweisen. Dem Administrator bzw. Sicherheitsbeauftragten bietet die Protokollierung auch eine Hilfe, um irrtümlich verwehrte Benutzerrechte ausfindig zu machen und zu korrigieren.

SafeGuard Enterprise protokolliert alle Aktivitäten und Statusinformationen der Endpoints sowie Administratoraktionen und sicherheitsrelevante Ereignisse und speichert diese zentral. Die Protokollierung zeichnet Ereignisse auf, die installierte SafeGuard Produkte auslösen. Die Art des Protokolls wird in Richtlinien vom Typ **Protokollierung** definiert. Hier legen Sie auch den fest, wo die protokollierten Ereignisse ausgegeben und gespeichert werden sollen: in der Windows-Ereignisanzeige des Endpoint oder in der SafeGuard Enterprise Datenbank.

Als Sicherheitsbeauftragter mit den entsprechenden Rechten können Sie die im SafeGuard Management Center angezeigten Statusinformationen und Protokollberichte einsehen, ausdrucken und archivieren. Umfassende Sortier- und Filterfunktionen unterstützen Sie im SafeGuard Management Center bei der Auswahl relevanter Ereignisse aus den verfügbaren Informationen.

Auch eine automatisierte Auswertung der Log-Datenbank, zum Beispiel über Crystal Reports oder Microsoft System Center Operations Manager, ist möglich. Die Protokolleinträge werden von SafeGuard Enterprise sowohl auf Client- als auch auf Server-Seite durch Signatur gegen unbefugte Manipulation geschützt.

Gemäß der Protokollierungsrichtlinie können Ereignisse aus den folgenden Kategorien protokolliert werden:

- Authentisierung
- Administration
- System
- Verschlüsselung
- Client
- Zugriffskontrolle
- Für **SafeGuard Data Exchange** lässt sich der Dateizugriff auf Wechselmedien durch Protokollierung der relevanten Ereignisse verfolgen. Weitere Informationen zu diesem Berichtstyp finden Sie unter Datei-Tracking-Bericht für Wechselmedien und Cloud-Speicher (Seite 275).
- Für **SafeGuard Cloud Storage** lässt sich der Zugriff auf Dateien in Ihrem Cloud-Speicher durch Protokollierung der relevanten Ereignisse verfolgen. Weitere Informationen zu diesem Berichtstyp finden Sie unter Datei-Tracking-Bericht für Wechselmedien und Cloud-Speicher (Seite 275).

33.1 Anwendungsgebiete

Die SafeGuard Enterprise Protokollierung von Ereignissen ist eine benutzerfreundliche und umfassende Lösung zum Aufzeichnen und Auswerten von Ereignissen. Die folgenden Beispiele zeigen einige typische Anwendungsszenarien für SafeGuard Enterprise **Berichte**.

33.1.1 Zentrale Überwachung von Endpoints im Netzwerk

Der Sicherheitsbeauftragte will regelmäßig über kritische Ereignisse (zum Beispiel Zugriff auf Dateien, für die ein Benutzer keine Berechtigung hat, oder eine Reihe von fehlgeschlagenen Anmeldeversuchen innerhalb eines bestimmten Zeitraums) informiert werden. Über eine Protokollierungsrichtlinie lässt sich die Protokollierung so konfigurieren, dass alle auf den relevanten Endpoints auftretenden sicherheitskritischen Ereignisse in einer lokalen Protokolldatei protokolliert. Nach Erreichen einer festgelegten Anzahl an Ereignissen wird die Protokolldatei über den SafeGuard Enterprise Server in die SafeGuard Enterprise Datenbank übertragen. In der **Ereignisanzeige** des SafeGuard Management Centers kann der Sicherheitsbeauftragte die Ereignisse abrufen, einsehen und analysieren. Somit lassen sich die Vorgänge auf den verschiedenen Endpoints kontrollieren, ohne dass Mitarbeiter Einfluss auf die Aufzeichnungen nehmen können.

33.1.2 Überwachen mobiler Benutzer

Mobile Benutzer sind in der Regel nicht ständig mit dem Unternehmensnetzwerk verbunden. Ein Außendienstmitarbeiter nimmt zum Beispiel für einen Termin sein Notebook vom Netz. Sobald er sich wieder am Netzwerk anmeldet, werden die während der Offline-Zeit protokollierten SafeGuard Enterprise Ereignisse übertragen. Die Protokollierung liefert somit einen genauen Überblick über die Benutzeraktivitäten während der betreffende Computer nicht an das Netzwerk angeschlossen war.

33.2 Voraussetzung

Ereignisse werden durch den SafeGuard Server verarbeitet. Wenn Sie auf Computern, auf denen kein SafeGuard Enterprise-Client installiert ist (SafeGuard Management Center-Computer oder der SafeGuard Enterprise Server selbst), Berichte aktivieren, müssen Sie sicherstellen, dass Ereignisse an den SafeGuard Enterprise Server gesendet werden. Sie müssen daher ein Client-Konfigurationspaket auf dem Computer installieren. Dadurch wird der Computer beim SafeGuard Enterprise Server als Client aktiviert und die Windows oder SafeGuard Enterprise Protokollierungsfunktionalität kann genutzt werden.

Weitere Informationen zu Client-Konfigurationspaketen finden Sie unter Mit Konfigurationspaketen arbeiten (Seite 100).

33.3 Ziel für protokollierte Ereignisse

Ziel der protokollierten Ereignisse kann die Windows-Ereignisanzeige oder die SafeGuard Enterprise Datenbank sein. In das jeweilige Ziel schreibt die Protokollierung nur Ereignisse, die mit einem SafeGuard-Produkt verknüpft sind.

Die Ausgabeziele für zu protokollierende Ereignisse werden in der Protokollierungsrichtlinie festgelegt.

33.3.1 Windows-Ereignisanzeige

Ereignisse, für die Sie in der Protokollierungsrichtlinie die Windows-Ereignisanzeige als Ziel festlegen, werden in der Windows-Ereignisanzeige abgelegt. Über die Windows-Ereignisanzeige lassen sich Protokolle für System-, Sicherheits- und Anwendungs-Ereignisse anzeigen und verwalten. Sie können diese Ereignisprotokolle auch speichern. Für diese Vorgänge benötigen Sie einen Administrator-Account für den jeweiligen Endpoint. In der Ereignisanzeige wird jeweils ein Fehlercode, kein beschreibender Text des Ereignisses, angezeigt.

Hinweis: Eine Voraussetzung, um SafeGuard Enterprise Events in der Windows Ereignisanzeige sehen zu können, ist, dass ein Client config.msi am Endpoint installiert ist.

Hinweis: Dieses Kapitel beschreibt das Einsehen sowie die Verwaltung und Analyse der Ereignisprotokolle im SafeGuard Management Center. Weitere Informationen zur Windows-Ereignisanzeige finden Sie in Ihrer Microsoft-Dokumentation.

33.3.2 SafeGuard Enterprise Datenbank

Ereignisse, für die Sie in der Protokollierungsrichtlinie die SafeGuard Enterprise Datenbank als Ziel festlegen, werden in lokalen Protokolldateien im Local Cache des jeweiligen Endpoint im Verzeichnis auditing\SGMTranslog gesammelt. Diese Dateien werden an den Transportmechanismus übergeben, der sie dann über den SafeGuard Enterprise Server in die Datenbank einträgt. Die Übergabe erfolgt standardmäßig immer dann, wenn der Transportmechanismus erfolgreich eine Verbindung zum Server aufbauen konnte. Um die Größe einer Protokolldatei einzuschränken, können Sie in einer Richtlinie des Typs **Allgemeine Einstellungen** eine maximale Anzahl an Protokolleinträgen definieren. Die Protokolldatei wird dann vom Protokollsystem nach Erreichen der festgelegten Anzahl an Einträgen in die Transportqueue des SafeGuard Enterprise Servers gestellt. Die in der zentralen Datenbank protokollierten Ereignisse lassen sich in der SafeGuard Enterprise **Ereignisanzeige** oder in der **Datei-Tracking-Anzeige** abrufen. Für das Einsehen, Analysieren und Verwalten der in der Datenbank protokollierten Ereignisse benötigen Sie als Sicherheitsbeauftragter die relevanten Berechtigungen.

33.4 Konfigurieren von Einstellungen für die Protokollierung

Die Definition von Berichten erfolgt über zwei Richtlinien:

- Richtlinie des Typs **Allgemeine Einstellungen**

  In einer Richtlinie des Typs **Allgemeine Einstellungen** können Sie die Anzahl an protokollierten Ereignissen angeben, nach deren Erreichen die Protokolldatei mit den für die zentrale Datenbank bestimmten Ereignissen an die SafeGuard Enterprise Datenbank übermittelt werden soll. Dadurch wird die Größe der einzelnen zu übertragenden Protokolldateien begrenzt. Diese Einstellung ist optional.

- Richtlinie des Typs **Protokollierung**

  Die zu protokollierenden Ereignisse werden in der Protokollierungsrichtlinie definiert. Hier legen Sie als Sicherheitsbeauftragter mit den relevanten Berechtigungen fest, welche Ereignisse an welchem Ausgabeort protokolliert werden.

33.4.1 Festlegen der Anzahl an Ereignissen für Rückmeldung

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Legen Sie eine neue Richtlinie des Typs **Allgemeine Einstellung** an oder wählen Sie eine bereits bestehende Richtlinie aus.
3. Legen Sie im Feld **Rückmeldung nach Anzahl von Ereignissen** unter **Protokollierung** die maximale Anzahl an Ereignissen pro Protokolldatei fest
4. Speichern Sie Ihre Einstellungen.

Nach dem Zuweisen der Richtlinie gilt die angegebene Anzahl an Ereignissen.

33.4.2 Auswahl von Ereignissen

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Legen Sie eine neue Richtlinie des Typs **Protokollierung** an oder wählen Sie eine bereits bestehende Richtlinie aus.

   Im rechten Aktionsbereich unter **Protokollierung** werden die vordefinierten Ereignisse, die protokolliert werden können, angezeigt. Standardmäßig werden Ereignisse nach **Ebene** gruppiert, zum Beispiel **Warnung** oder **Fehler**. Sie können die Gruppierung jedoch ändern. Ein Klick auf die Spaltenüberschrift sortiert die Ereignisse nach **ID**, **Kategorie** usw.

3. Um festzulegen, dass ein Ereignis in der SafeGuard Enterprise Datenbank protokolliert werden soll, wählen Sie das Ereignis in der Spalte mit dem Datenbanksymbol **Ereignisse in der Datenbank protokollieren** durch Klicken mit der Maus aus. Für Ereignisse, die in der Windows-Ereignisanzeige protokolliert werden sollen, klicken Sie in der Spalte mit dem Ereignisprotokollsymbol **Im Ereignisprotokoll protokollieren**.

   Durch wiederholtes Klicken lässt sich die Markierung wieder aufheben oder auf null setzen. Für Ereignisse, für die Sie keine Einstellung festlegen, gelten die vordefinierten Standardwerte.

4. Bei den für die Protokollierung ausgewählten Ereignissen wird in der betreffenden Spalte ein grünes Häkchen angezeigt. Speichern Sie Ihre Einstellungen.

Nach der Zuweisung der Richtlinie werden die ausgewählten Ereignisse am festgelegten Ausgabeziel protokolliert.

Hinweis: Eine Auflistung aller für die Protokollierung auswählbaren Ereignisse finden Sie unter Für Berichte auswählbare Ereignisse (Seite 298).

33.5 Einsehen von protokollierten Ereignissen

Wenn Sie als Sicherheitsbeauftragter über die entsprechenden Berechtigungen verfügen, können Sie die in der zentralen Datenbank protokollierten Ereignisse in der SafeGuard Management Center **Ereignisanzeige** einsehen.

So rufen Sie in der zentralen Datenbank protokollierte Ereignisse ab:

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf die Schaltfläche **Berichte**.
2. Markieren Sie im **Berichte** Navigationsbereich den Eintrag **Ereignisanzeige**.
3. Klicken Sie im rechten Fensterbereich **Ereignisanzeige** auf das Lupensymbol.

Alle in der zentralen Datenbank protokollierten Ereignisse werden in der **Ereignisanzeige** angezeigt.

Die einzelnen Spalten zeigen folgende Informationen zu den protokollierten Ereignissen:

Spalte	Beschreibung
ID	Zeigt eine Nummer zur Identifizierung des Ereignisses.
Ereignis	Zeigt den Ereignistext, d.h. eine Beschreibung des Ereignisses.
Kategorie	Zeigt die Klassifizierung des Ereignisses durch die Quelle, z. B.:Verschlüsselung, Anmeldung, System.
Anwendung	Zeigt den Bereich der Software, der das Ereignis übermittelt hat, z. B. SGMAuth, SGBaseENc, SGMAS.
Computer	Zeigt den Namen des Computers, auf dem das protokollierte Ereignis aufgetreten ist.
Computerdomäne	Zeigt die Domäne des Computers, auf dem das protokollierte Ereignis aufgetreten ist.
Benutzer	Zeigt den Benutzer, der beim Auftreten des Ereignisses angemeldet war.
Benutzerdomäne	Zeigt die Domäne des Benutzers, der beim Auftreten des Ereignisses angemeldet war.
Zeitpunkt der Protokollierung	Zeigt Systemdatum und Systemuhrzeit der Protokollierung des Ereignisses auf dem Endpoint.

Durch Klicken auf den Spalten-Header lässt sich die Ereignisanzeige nach **Ebene**, **Kategorie** usw. sortieren.

Darüber hinaus steht über das Kontextmenü der einzelnen Spalten eine Reihe von Funktionen für die Sortierung, Gruppierung und Anpassung der Ereignisanzeige zur Verfügung.

Wenn Sie auf einen Eintrag in der **Ereignisanzeige** doppelklicken, werden Details zum protokollierten Ereignis angezeigt.

33.5.1 Filtern der SafeGuard Enterprise Ereignisanzeige

Das SafeGuard Management Center bietet umfassende Filterfunktionen. Mit diesen Funktionen können Sie die jeweils relevanten Ereignisse schnell aus Fülle der in der Ereignisanzeige dargestellten Informationen ermitteln.

Im **Filter**-Bereich der **Ereignisanzeige** stehen folgende Felder für die Definition von Filtern zur Verfügung:

Feld	Beschreibung
Kategorien	Unter Anwendung dieses Felds lässt sich die **Ereignisanzeige** nach den in der Spalte **Kategorie** angegebenen Klassifizierungen durch die Quelle (zum Beispiel **Verschlüsselung**, **Anmeldung**, **System**) filtern. Wählen Sie hierzu die gewünschten Kategorien in der Dropdownliste des Felds aus.
Fehlerstufe	Unter Anwendung dieses Felds lässt sich die **Ereignisanzeige** nach den in der Spalte **Ebene** angegebenen Windows-Ereignisklassifizierungen (z. B. Warnung, Fehler) filtern. Wählen Sie hierzu die gewünschten Ebenen in der Dropdownliste des Felds aus.
Zeige letzte	In diesem Feld können Sie die Anzahl der anzuzeigenden Ereignisse festlegen. Es werden jeweils die zuletzt protokollierten Ereignisse (standardmäßig die 100 letzten Ereignisse) angezeigt.

Darüber hinaus können Sie mit dem Filter-Editor benutzerdefinierte Filter erstellen. Der Filter-Editor lässt sich über das Kontextmenü der einzelnen Berichtsspalten aufrufen. Im Fenster **Filterdefinition** können Sie eigene Filter definieren und auf die jeweilige Spalte anwenden.

33.6 Datei-Tracking-Bericht für Wechselmedien und Cloud-Speicher

Bei **SafeGuard Data Exchange** und **SafeGuard Cloud Storage** lässt sich der Zugriff auf Dateien auf Wechselmedien oder in Ihrem Cloud-Speicher protokollieren. Unabhängig davon, ob eine Verschlüsselungsrichtlinie für Dateien auf Wechselmedien oder Cloud-Speicher gilt, lassen sich Ereignisse für folgende Aktionen protokollieren:

- Auf einem Wechselmedium oder im Cloud-Speicher wird eine Datei oder ein Verzeichnis angelegt.
- Auf einem Wechselmedium oder im Cloud-Speicher wird eine Datei oder ein Verzeichnis umbenannt.
- Auf einem Wechselmedium oder im Cloud-Speicher wird eine Datei oder ein Verzeichnis gelöscht.

Sie können die Events für den Dateizugriff in der Windows Ereignisanzeige oder in der SafeGuard Enterprise **Datei-Tracking-Anzeige** einsehen, je nachdem, welches Ziel Sie bei der Definition der Protokollierungsrichtlinie angeben.

33.6.1 Konfigurieren von Datei-Tracking

1. Klicken Sie im SafeGuard Management Center auf **Richtlinien**.
2. Legen Sie eine neue Richtlinie des Typs **Protokollierung** an oder wählen Sie eine bereits bestehende Richtlinie aus.

   Im rechten Aktionsbereich unter **Protokollierung** werden die vordefinierten Ereignisse, die protokolliert werden können, angezeigt. Ein Klick auf die Spaltenüberschrift sortiert die Ereignisse nach **ID**, **Kategorie** usw.

3. Um die Protokollierung des Dateizugriffs zu aktivieren, wählen Sie je nach Anforderung die folgenden Ereignisse:
   - Für Dateien, die auf Wechselmedien gespeichert sind:
     - ID 3020 Datei-Tracking für Wechselmedien: Eine Datei wurde erstellt.
     - ID 3021 Datei-Tracking für Wechselmedien: Eine Datei wurde umbenannt.
     - ID 3022 Datei-Tracking für Wechselmedien: Eine Datei wurde gelöscht.
   - Für Dateien, die im Cloud-Speicher gespeichert sind:
     - ID 3025 Datei-Tracking für Cloud-Speicher: Eine Datei wurde erstellt.
     - ID 3026 Datei-Tracking für Cloud-Speicher: Eine Datei wurde umbenannt.
     - ID 3027 Datei-Tracking für Cloud-Speicher: Eine Datei wurde gelöscht.

   Um festzulegen, dass ein Ereignis in der SafeGuard Enterprise Datenbank protokolliert werden soll, wählen Sie das Ereignis in der Spalte mit dem Datenbanksymbol **Ereignisse in der Datenbank protokollieren** durch Klicken mit der Maus aus. Für Ereignisse, die in der Windows-Ereignisanzeige protokolliert werden sollen, klicken Sie in der Spalte mit dem Ereignisprotokollsymbol **Im Ereignisprotokoll protokollieren**.

   Bei den für die Protokollierung ausgewählten Ereignissen wird in der betreffenden Spalte ein grünes Häkchen angezeigt.
4. Speichern Sie Ihre Einstellungen.

Nach dem Zuweisen der Richtlinie ist Datei-Tracking aktiviert und die ausgewählten Ereignisse werden am ausgewählten Zielort protokolliert.

Hinweis: Beachten Sie, dass sich durch das Aktivieren von Datei-Tracking die Serverlast erheblich erhöht.

33.6.2 Einsehen von Datei-Tracking-Ereignissen

Um Datei-Tracking-Protokolle einzusehen, benötigen Sie das Recht **Datei-Tracking-Ereignisse anzeigen**.

1. Klicken Sie im Navigationsbereich des SafeGuard Management Center auf die Schaltfläche **Berichte**.
2. Markieren Sie im **Berichte** Navigationsbereich den Eintrag **Datei-Tracking-Anzeige**.
3. Klicken Sie im Aktionsbereich der **Datei-Tracking-Anzeige** auf der rechten Seite auf das Lupensymbol.

Alle in der zentralen Datenbank protokollierten Ereignisse werden in der **Datei-Tracking-Anzeige** angezeigt. Die Ansicht ist mit der Ansicht der **Ereignisanzeige** identisch. Weitere Informationen finden Sie unter Einsehen von protokollierten Ereignissen (Seite 273).

33.7 Drucken von Berichten

Die in der SafeGuard Management Center **Ereignisanzeige** oder in der **Datei-Tracking-Anzeige** angezeigten Ereignisberichte lassen sich über das **Datei** Menü in der Menüleiste des SafeGuard Management Center drucken.

- Um vor dem Drucken eine Druckvorschau zu erstellen, wählen Sie **Datei > Druckvorschau**. In der Druckvorschau stehen verschiedene Funktionen, zum Beispiel für den Export des Dokuments in eine Reihe von Ausgabeformaten (zum Beispiel .PDF) oder die Bearbeitung des Seitenlayouts (zum Beispiel Kopf- und Fußzeile), zur Verfügung.
- Um das Dokument sofort zu drucken, wählen Sie **Datei > Drucken**.

33.8 Verkettung von protokollierten Ereignissen

Die für die zentrale Datenbank bestimmten Ereignisse werden in der EVENT-Tabelle der SafeGuard Enterprise Datenbank protokolliert. Auf diese Tabelle kann ein spezieller Integritätsschutz angewendet werden. Die Ereignisse lassen sich als verkettete Liste in der EVENT-Tabelle protokollieren. Durch die Verkettung ist ein Eintrag in der Liste jeweils von seinem Vorgängereintrag abhängig. Wird ein Eintrag aus der Liste entfernt, so ist dies sichtbar und über eine Integritätsprüfung nachweisbar.

Zur Optimierung der Performance ist die Verkettung der Ereignisse in der EVENT-Tabelle standardmäßig deaktiviert. Sie können zur Überprüfung der Integrität der protokollierten Ereignisse die Verkettung aktivieren (siehe Überprüfen der Integrität der protokollierten Ereignisse (Seite 278)).

Hinweis: Wenn die Verkettung von protokollierten Ereignissen deaktiviert ist, gilt kein spezieller Integritätsschutz für die EVENT-Tabelle.

Hinweis: Zu viele Events können zu Performanceproblemen führen. Weitere Informationen über die Vermeidung von Performanceproblemen durch Löschen von Ereignissen finden Sie unter Regelmäßige Säuberung der EVENT-Tabelle über Skript (Seite 279).

33.8.1 Aktivieren der Verkettung protokollierter Ereignisse

1. Stoppen Sie den Webservice SGNSRV auf dem Web Server.
2. Löschen Sie alle Ereignisse aus der Datenbank und erstellen Sie während des Löschvorgangs eine Sicherungskopie (siehe Löschen ausgewählter oder aller Ereignisse (Seite 278)).

   Hinweis: Wenn Sie die alten Ereignisse nicht aus der Datenbank löschen, funktioniert die Verkettung nicht, da für die verbleibenden alten Ereignisse die Verkettung nicht aktiviert war.

3. Setzen Sie folgenden Registry Key auf 0 oder löschen Sie ihn:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SafeGuard Enterprise DWORD:
   DisableLogEventChaining = 0
   ```

4. Starten Sie den Webservice neu.

Die Verkettung ist wieder aktiviert.

Hinweis: Um die Verkettung wieder zu deaktivieren, setzen Sie den Registry Key auf 1.

33.9 Prüfen der Integrität protokollierter Ereignisse

Voraussetzung: Für die Überprüfung der Integrität von protokollierten Ereignissen muss die Verkettung der Ereignisse in der EVENT-Tabelle aktiviert sein.

1. Klicken Sie im SafeGuard Management Center auf **Berichte**.
2. Wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen > Integrität prüfen**.

Eine Meldung liefert die Informationen zur Integrität der protokollierten Ereignisse.

Hinweis: Ist die Verkettung von Ereignissen deaktiviert, so wird ein Fehler ausgegeben.

33.10 Löschen ausgewählter oder aller Ereignisse

1. Klicken Sie im SafeGuard Management Center auf **Berichte**.
2. Markieren Sie in der **Ereignisanzeige** die Ereignisse, die gelöscht werden sollen.
3. Um ausgewählte Ereignisse zu löschen, wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen > Ereignisse löschen** oder klicken Sie in der Symbolleiste auf das Symbol **Ausgewählte Ereignisse löschen**. Um alle Ereignisse zu löschen, wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen > Alle Ereignisse löschen** oder klicken Sie in der Symbolleiste auf das Symbol **Alle Ereignisse löschen**.
4. Vor dem Löschen der ausgewählten Ereignisse wird das Fenster **Ereignisse sichern als** zum Erstellen einer Sicherungsdatei angezeigt (siehe Erstellen einer Sicherungsdatei (Seite 278)).

Die ausgewählten Ereignisse werden aus dem Ereignisprotokoll gelöscht.

33.11 Erstellen einer Sicherungsdatei

Sicherungsdateien von den in der Ereignisanzeige angezeigten Berichten lassen sich im Rahmen des Löschvorgangs erstellen.

1. Wenn Sie **Aktionen > Ereignisse löschen** oder **Aktionen > Alle Ereignisse löschen** wählen, wird vor dem Löschen der Ereignisse das Fenster **Ereignisse sichern als** zur Erstellung einer Sicherungsdatei angezeigt.
2. Um eine Sicherung des Ereignisprotokolls in Form einer XML-Datei zu erstellen, geben Sie einen Dateinamen und einen Speicherort an und klicken Sie auf **OK**.

33.12 Öffnen einer Sicherungsdatei

1. Klicken Sie im SafeGuard Management Center auf **Berichte**.
2. Wählen Sie in der SafeGuard Management Center Menüleiste **Aktionen > Sicherungsdatei öffnen**.

   Das Fenster **Sicherung öffnen** wird angezeigt.

3. Wählen Sie die zu öffnende Sicherungsdatei aus und klicken Sie auf **Öffnen**.

Die Sicherungsdatei wird geöffnet und die Ereignisse werden in der **Ereignisanzeige** angezeigt. Um wieder zur regulären Ansicht der **Ereignisanzeige** zurückzukehren, klicken Sie erneut auf das Symbol **Sicherungsdatei öffnen** in der Symbolleiste.

33.13 Regelmäßige Säuberung der EVENT-Tabelle über Skript

Hinweis: Das SafeGuard Management Center bietet den **Taskplaner** für das Erstellen und Planen von auf Skripten basierenden Tasks, die in regelmäßigen Abständen ausgeführt werden. Auf dem SafeGuard Enterprise Server startet ein Service die Tasks automatisch zur Ausführung der angegebenen Skripte.

Für die automatische und effiziente Säuberung der EVENT-Tabelle stehen im \tools Verzeichnis Ihrer SafeGuard Enterprise Software-Lieferung vier SQL Skripte zur Verfügung:

- **spShrinkEventTable_install.sql**
- **ScheduledShrinkEventTable_install.sql**
- **spShrinkEventTable_uninstall.sql**
- **ScheduledShrinkEventTable_uninstall.sql**

Die beiden Skripte **spShrinkEventTable_install.sql** und **ScheduledShrinkEventTable_install.sql** installieren eine gespeicherte Prozedur sowie den Scheduled Job auf dem Datenbank-Server. Der Scheduled Job führt die gespeicherte Prozedur in festgelegten, regelmäßigen Abständen aus. Die gespeicherte Prozedur verschiebt Ereignisse aus der EVENT-Tabelle in die Backup-Log-Tabelle EVENT_BACKUP. Dabei wird eine definierte Anzahl an neuesten Ereignissen in der EVENT-Tabelle belassen.

Die beiden Skripte **spShrinkEventTable_uninstall.sql** und **ScheduledShrinkEventTable_uninstall.sql** deinstallieren die gespeicherte Prozedur sowie den Scheduled Job. Diese beiden Skripte löschen auch die EVENT_BACKUP Tabelle.

Hinweis: Wenn Sie die Ereignisse über die gespeicherte Prozedur aus der EVENT-Tabelle in die Backup-Log-Tabelle verschieben, findet die Verkettung der Protokollierung keine Anwendung mehr. Es ist nicht sinnvoll, die Verkettung zu aktivieren und gleichzeitig die gespeicherte Prozedur zur Säuberung der EVENT-Tabelle einzusetzen. Weitere Informationen finden Sie unter Verkettung von protokollierten Ereignissen (Seite 277).

33.13.1 Erstellen der gespeicherten Prozedur

Das Skript **spShrinkEventTable_install.sql** erstellt eine gespeicherte Prozedur, die Daten aus der EVENT-Tabelle in eine Backup-Log-Tabelle mit dem Namen EVENT_BACKUP verschiebt. Wenn die Tabelle EVENT_BACKUP noch nicht vorhanden ist, wird sie automatisch erstellt.

Die erste Zeile lautet „USE SafeGuard“. Wenn Sie für Ihre SafeGuard Enterprise Datenbank einen anderen Namen als „SafeGuard“ verwendet haben, ändern Sie den Namen hier entsprechend.

Die gespeicherte Prozedur belässt die **<n>** neuesten Ereignisse in der EVENT-Tabelle und verschiebt den Rest in die Tabelle EVENT_BACKUP. Die Anzahl an Ereignissen, die in der EVENT-Tabelle verbleiben sollen, wird über einen Parameter festgelegt.

Um die gespeicherte Prozedur auszuführen, verwenden Sie folgenden Befehl in SQL Server Management Studio (New Query):

```
exec spShrinkEventTable 1000
```

Bei Verwendung dieses Beispielbefehls werden alle Ereignisse außer den neuesten 1000 verschoben.

33.13.2 Anlegen eines Scheduled Job für die Ausführung der gespeicherten Prozedur

Um die EVENT-Tabelle in regelmäßigen Abständen automatisch zu säubern, können Sie einen Job am SQL Server anlegen. Dieser Job kann über das Skript **ScheduledShrinkEventTable_install.sql** oder über den SQL Enterprise Manager erstellt werden.

Hinweis: Der Job funktioniert nicht bei SQL Express Datenbanken. Damit der Job ausgeführt werden kann, muss der SQL Server Agent laufen. Da bei SQL Server Express Installation kein SQL Server Agent vorhanden ist, werden Jobs hier nicht unterstützt.

- Der Skript-Teil muss in der msdb ausgeführt werden. Wenn Sie für Ihre SafeGuard Enterprise Datenbank einen anderen Namen als SafeGuard ausgewählt haben, ändern Sie den Namen entsprechend.

  ```
  /* Default: Database name 'SafeGuard' change if required*/
  SELECT @SafeGuardDataBase='SafeGuard'
  ```

- Sie können auch die Anzahl an Ereignissen festlegen, die in der EVENT-Tabelle verbleiben sollen. Die Standardeinstellung ist 100.000.

  ```
  /* Default: keep the latest 100000 events, change if required*/
  SELECT @ShrinkCommand='exec spShrinkEventTable 100000'
  ```

- Sie können festlegen, ob die Ausführung des Jobs im NT Event Log protokolliert werden soll.

  ```
  exec sp_add_job
  @job_name='AutoShrinkEventTable',
  @enabled=1,
  @notify_level_eventlog=3
  ```

  Für den Parameter **notify_level_eventlog** sind folgende Werte verfügbar:

Wert	Ergebnis
3	Jede Ausführung des Jobs protokollieren.
2	Fehlschlagen des Jobs protokollieren.
1	Erfolgreiche Ausführung des Jobs protokollieren.
0	Ausführung des Jobs nicht im NT Event Log protokollieren.

- Sie können festlegen, wie oft die Ausführung des Jobs im Fall eines Fehlschlags wiederholt werden soll.

exec sp_add_jobstep

- **@retry_attempts=3**

  Dieses Beispiel legt 3 Versuche für die Ausführung des Jobs im Fall eines Fehlschlags fest.

- **@retry_interval=60**

  Dieses Beispiel legt fest, dass die Ausführung des Jobs in einem Abstand von 60 Minuten wiederholt werden soll.

- Sie können einen Zeitplan für die Ausführung des Jobs festlegen.

  exec sp_add_jobschedule

  - **@freq_type=4**

    Dieses Beispiel legt fest, dass der Job täglich ausgeführt wird.

  - **@freq_interval=1**

    Dieses Beispiel legt fest, dass der Job einmal pro Tag ausgeführt wird.

  - **@active_start_time=010000**

    Dieses Beispiel legt fest, dass der Job um 01:00 Uhr ausgeführt wird.

Hinweis: Neben den oben angeführten Beispielwerten lässt sich noch eine Vielzahl von verschiedenen Zeitplanoptionen mit **sp_add-jobschedule** definieren. So lässt sich der Job zum Beispiel alle zwei Minuten oder nur einmal pro Woche ausführen. Weitere Informationen hierzu finden Sie in der Microsoft Transact SQL Dokumentation.

33.13.3 Löschen der gespeicherten Prozeduren, Jobs und Tabellen

Das Skript **spShrinkEventTable_uninstall.sql** löscht die gespeicherte Prozedur sowie die EVENT-BACKUP Tabelle. Das Skript **ScheduledShrinkEventTable_uninstall.sql** deaktiviert den Scheduled Job.

Hinweis: Wenn Sie **spShrinkEventTable_uninstall.sql** ausführen, wird die Tabelle EVENT_BACKUP mit allen enthaltenen Daten vollständig gelöscht.

33.14 Texte für Ereignisberichte

Ereignisse werden nicht mit ihren vollständigen Ereignistexten in der SafeGuard Enterprise Datenbank protokolliert. Nur die ID und die relevanten Parameterwerte werden in die Datenbanktabelle geschrieben. Beim Abrufen der Ereignisse in der SafeGuard Management Center **Ereignisanzeige** werden die Parameterwerte zusammen mit den in der .dll enthaltenen Lückentexten in die kompletten Ereignistexte umgesetzt. Dies erfolgt in der jeweils benutzten Systemsprache des SafeGuard Management Center.

Die für die Ereignistexte verwendeten Lückentexte lassen sich, zum Beispiel durch SQL-Abfragen, bearbeiten und aufbereiten. Sie können hierzu eine Tabelle mit allen Lückentexten für Ereignismeldungen erzeugen. Danach können Sie die Lückentexte nach Ihren Anforderungen anpassen.

So erstellen Sie eine Tabelle mit den Texten für die einzelnen Ereignis-IDs:

1. Wählen Sie in der Menüleiste des SafeGuard Management Center **Extras > Optionen**.

2. Wählen Sie in der Menüleiste des SafeGuard Management Centers **Extras > Optionen**.
3. Klicken Sie im Bereich **Texte für Ereignisberichte** auf die Schaltfläche **Erzeuge Tabelle**.

Die Tabelle mit den Texten für die Bericht IDs wird in der jeweils aktuellen Sprache des SafeGuard Management Centers erstellt und kann angepasst werden.

Hinweis: Vor jedem neuen Erstellen der Lückentexte wird die Tabelle jeweils geleert. Wenn die Texte für eine Sprache wie beschrieben erstellt wurden und ein Benutzer erstellt die Texte für eine andere Sprache, so werden die Texte für die erste Sprache entfernt.

34 Planen von Tasks

Das SafeGuard Management Center bietet den **Taskplaner** für das Erstellen und Planen von auf Skripten basierenden Tasks, die in regelmäßigen Abständen ausgeführt werden. Auf dem SafeGuard Enterprise Server startet ein Service die Tasks automatisch zur Ausführung der angegebenen Skripte.

Periodische Tasks sind z. B. nützlich für

- die automatische Synchronisierung zwischen dem Active Directory und SafeGuard Enterprise.
- das automatische Löschen von protokollierten Ereignissen.

Für diese beiden Vorgänge stehen in SafeGuard Enterprise vordefinierte Skripte zur Verfügung. Sie können diese Skripte unverändert verwenden oder Ihren Anforderungen anpassen. Weitere Informationen finden Sie unter Vordefinierte Skripte für regelmäßig wiederkehrende Tasks (Seite 289).

Als Sicherheitsbeauftragter mit den erforderlichen Rechten können Sie Skripte, Regeln und zeitliche Intervalle für die Tasks im **Taskplaner** definieren.

Hinweis: Stellen Sie sicher, dass für das Konto, das für die Verwendung des SafeGuard Enterprise **Taskplaners** benutzt wird, die geeigneten SQL-Berechtigungen eingestellt sind. Weitere Informationen hierzu finden Sie in unserer Wissensdatenbank: http://www.sophos.com/de-de/support/knowledgebase/113582.aspx.

Hinweis: Die API kann nicht mehrere Tasks gleichzeitig verarbeiten. Wenn Sie mehrere Konten pro Task verwenden, führt dies zu Datenbankzugriffsverletzungen.

34.1 Erstellen eines neuen Tasks

Um Tasks im **Taskplaner** zu erstellen, benötigen Sie die Sicherheitsbeauftragtenrechte **Taskplaner benutzen** und **Tasks verwalten**.

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** wird angezeigt.

2. Klicken Sie auf die Schaltfläche **Erzeugen...**

   Der Dialog **Neuer Task** wird angezeigt.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für den Task ein.

   Ist der Task-Name nicht eindeutig, so wird eine Warnungsmeldung angezeigt, wenn Sie auf **OK** klicken, um den Task zu speichern.

4. Wählen Sie aus der Dropdownliste des Felds **SGN Server** den Server, auf dem der Task laufen soll.

   Die Dropdownliste zeigt nur Server, für die die Skript-Ausführung erlaubt ist. Sie können die Skript-Ausführung für einen bestimmten Server als erlaubt definieren, wenn Sie diesen mit der Funktion **Konfigurationspakete** im SafeGuard Management Center registrieren. Weitere Informationen zum Registrieren von Servern finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

   Wenn Sie **Keiner** auswählen, wird der Task nicht ausgeführt.

5. Klicken Sie auf die Dropdown-Schaltfläche **Importieren...** neben dem Feld **Skript**.

   Der Dialog **Skript-Datei für den Import auswählen** wird angezeigt.

   Hinweis: Im Verzeichnis Script Templates Ihrer SafeGuard Management Center Installation stehen zwei vordefinierte Skripte zur Verfügung. Der Dialog **Skript-Datei für den Import auswählen** zeigt automatisch dieses Verzeichnis an. Weitere Informationen finden Sie unter Vordefinierte Skripte für regelmäßig wiederkehrende Tasks (Seite 289).

   Mit dem **Taskplaner** können Sie Skripte importieren, exportieren und bearbeiten. Weitere Informationen finden Sie unter Mit Skripten im Task Scheduler arbeiten (Seite 287).

6. Wählen Sie das Skript aus, das mit dem Task ausgeführt werden soll, und klicken Sie auf **OK**.

   Wenn das ausgewählte Skript leer ist, bleibt die Schaltfläche **OK** im Dialog deaktiviert. Außerdem wird ein Warnungssymbol angezeigt.

7. Geben Sie im Feld **Startzeit** an, wann der Task auf dem ausgewählten Server ausgeführt werden soll.

   Die Startzeit wird unter Anwendung der lokalen Zeit des Computers, auf dem das SafeGuard Management Center läuft, angegeben. Intern wird die Startzeit als Coordinated Universal Time (UTC) gespeichert. Dadurch können Tasks auch dann exakt zur gleichen Zeit ausgeführt werden, wenn sich Server in unterschiedlichen Zeitzonen befinden. Alle Server verwenden die aktuelle Zeit des Datenbankservers für das Starten von Tasks. Zur Optimierung der Task-Überwachung wird die Datenbankreferenzzeit im **Taskplaner** Dialog angezeigt.

8. Geben Sie im Feld **Wiederholung** an, wie oft der Task auf dem ausgewählten Server ausgeführt werden soll.

   - Um den Task einmal auszuführen, wählen Sie **Einmal** und geben Sie das gewünschte **Datum** an.
   - Um den Task täglich auszuführen, wählen Sie **Täglich** und dann **Jeden Tag (inklusive Samstag und Sonntag)** oder **Jeden Wochentag (Montag - Freitag)**.
   - Um den Task wöchentlich auszuführen, wählen Sie **Wöchentlich** und geben Sie den gewünschten Tag in der Woche an.
   - Um den Task monatlich auszuführen, wählen Sie **Monatlich** und geben Sie den gewünschten Tag im Monat aus einem Bereich von 1 bis 31 an. Um den Task am letzten Tag des Monats auszuführen, wählen Sie **Letzter** aus der Dropdownliste.

   Wenn Sie alle obligatorischen Felder ausgefüllt haben, wird die Schaltfläche **OK** aktiv.

9. Klicken Sie auf **OK**.

Der Task wird in der Datenbank gespeichert und in der **Taskplaner** Übersicht angezeigt. Er wird gemäß dem angegebenen Plan auf dem ausgewählten Server ausgeführt.

34.2 Die Taskplaner-Übersichtanzeige

Nachdem Sie Tasks zur Ausführung auf einem SafeGuard Enterprise Server erstellt haben, werden diese im Dialog **Taskplaner** angezeigt, den Sie über **Extras > Taskplaner** öffnen.

Dieser Dialog zeigt die folgenden Spalten für die einzelnen Tasks:

Spalte	Beschreibung
Task-Name	Zeigt den eindeutigen Task-Namen.
SGN Server	Gibt an, auf welchem Server der Task ausgeführt wird.
Geplante Ausführung	Zeigt den für den Task definierten Zeitplan inklusive Wiederholung und Zeit.
Nächste Ausführung	Zeigt an, wann der Task zum nächsten Mal ausgeführt wird (Datum und Uhrzeit). Wenn für diesen Task keine weiteren Ausführungen vorgesehen sind, wird in dieser Spalte **Keine** angezeigt.
Letzte Ausführung	Zeigt an, wann der Task zum letzten mal ausgeführt wurde (Datum und Uhrzeit). Wurde der Task noch nicht ausgeführt, so wird in dieser Spalte **Keine** angezeigt.
Ergebnis der letzten Ausführung	Zeigt das Ergebnis der letzten Task-Ausführung: ▪ **Erfolgreich** Das dem Task zugeordnete Skript wurde erfolgreich ausgeführt. ▪ **Fehlgeschlagen** Der Task konnte nicht ausgeführt werden. Falls verfügbar, wird eine Fehlernummer angezeigt. ▪ **Läuft** Das Skript läuft derzeit. ▪ **Unzureichende Berechtigung** Der Task ist aufgrund von unzureichender Berechtigung für die Skript-Ausführung fehlgeschlagen. ▪ **Abgebrochen** Die Task-Ausführung wurde abgebrochen, da die Zeitdauer 24 Stunden überschritten hat. ▪ **Steuerung nicht möglich** Die Steuerung der Ausführung des Skripts, das dem Task zugeordnet ist, war nicht möglich. Ein

Spalte	Beschreibung
	möglicher Grund hierfür ist z. B., dass der SGN Scheduler Service gestoppt wurde. ▪ **Beschädigtes Skript** Das auszuführende Skript ist beschädigt. ▪ **Skript inzwischen gelöscht** Während sich der Task in der Warteschlange für die Ausführung befand, wurde das Skript aus der SafeGuard Enterprise Datenbank entfernt. ▪ **Runtime-Fehler** Während der Verarbeitung des Scheduler Service ist ein Runtime-Fehler aufgetreten.

Unterhalb der Spalten befinden sich folgende Schaltflächen:

Schaltfläche	Beschreibung
Erzeugen...	Klicken Sie auf diese Schaltfläche, um einen neuen Task zu erstellen.
Löschen	Klicken Sie auf diese Schaltfläche, um einen ausgewählten Task zu löschen.
Eigenschaften	Klicken Sie auf diese Schaltfläche, um den **<Task-Name> Eigenschaften** Dialog für einen ausgewählten Task anzuzeigen. In diesem Dialog können Sie den Task bearbeiten oder Skripte importieren, exportieren und bearbeiten.
Aktualisieren	Klicken Sie auf diese Schaltfläche, um die Task-Liste im **Taskplaner** Dialog zu aktualisieren. Wenn ein Benutzer in der Zwischenzeit Tasks hinzugefügt oder gelöscht hat, wird die Task-Liste aktualisiert.

Alle Server verwenden die aktuelle Zeit des Datenbankservers für das Starten von Tasks. Um eine bessere Überwachung von Tasks zu gewährleisten wird hier die Zeit des Datenbankservers angezeigt. Diese wird unter Benutzung der lokalen Zeitzone des Computers, auf dem das SafeGuard Management Center läuft, angegeben.

34.3 Bearbeiten von Tasks

Um Tasks im **Taskplaner** zu bearbeiten, benötigen Sie die Sicherheitsbeauftragtenrechte **Taskplaner benutzen** und **Tasks verwalten**.

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** mit einer Übersicht über die geplanten Tasks wird angezeigt.

2. Wählen Sie den gewünschten Task und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Der **<Task-Name> Eigenschaften** Dialog mit den Eigenschaften des ausgewählten Tasks wird angezeigt.

3. Nehmen Sie die gewünschten Änderungen vor.

   Hinweis: Der Task-Name muss eindeutig sein. Wenn Sie den Namen in einen bereits vorhandenen Task-Namen ändern, wird eine Fehlermeldung angezeigt.

4. Klicken Sie auf **OK**.

Die Änderungen werden wirksam.

34.4 Löschen von Tasks

Um Tasks aus dem **Taskplaner** zu entfernen, benötigen Sie die Sicherheitsbeauftragtenrechte **Taskplaner benutzen** und **Tasks verwalten**.

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** mit einer Übersicht über die geplanten Tasks wird angezeigt.

2. Wählen Sie den gewünschten Task aus.

   Die Schaltfläche **Löschen** wird aktiv.

3. Klicken Sie auf die Schaltfläche **Löschen** und bestätigen Sie, dass Sie den Task löschen möchten.

Der Task wird aus der Übersicht des **Taskplaner** Dialogs entfernt und nicht mehr auf dem SafeGuard Enterprise Server ausgeführt.

Hinweis: Wurde der Task in der Zwischenzeit gestartet, so wird er zwar aus dem **Taskplaner** Übersichtsdialog entfernt, jedoch noch komplett ausgeführt.

34.5 Mit Skripten im Taskplaner arbeiten

Mit dem **Taskplaner** können Sie Skripte importieren, bearbeiten und exportieren. Um mit Skripten im **Taskplaner**zu arbeiten, benötigen Sie die Sicherheitsbeauftragtenrechte **Taskplaner benutzen** und **Tasks verwalten**.

34.5.1 Import von Skripts

Damit Sie ein Skript für die Ausführung mit einem Task angeben können, müssen Sie es importieren. Sie können das Skript beim Erstellen eines neuen Tasks importieren. Sie können auch Skripts für bereits vorhandene Tasks importieren.

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** mit einer Übersicht über die geplanten Tasks wird angezeigt.

2. Wählen Sie den gewünschten Task und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Der **<Task-Name> Eigenschaften** Dialog mit den Eigenschaften des ausgewählten Tasks wird angezeigt.

3. Klicken Sie auf die Dropdown-Schaltfläche **Importieren...** neben dem Feld **Skript**.

   Der Dialog **Skript-Datei für den Import auswählen** wird angezeigt.

   Hinweis: Im Verzeichnis Script Templates Ihrer SafeGuard Management Center Installation stehen zwei vordefinierte Skripte zur Verfügung. Der Dialog **Skript-Datei für den Import auswählen** zeigt automatisch dieses Verzeichnis an. Weitere Informationen finden Sie unter Vordefinierte Skripte für regelmäßig wiederkehrende Tasks (Seite 289).

4. Wählen Sie das zu importierende Skript aus und klicken Sie auf **OK**.

   Der Skript-Name wird im Feld **Skript** angezeigt.

5. Klicken Sie auf **OK**.

   Wenn das Skript bereits importiert wurde, werden Sie aufgefordert zu bestätigen, dass das alte Skript überschrieben werden soll.

   Wenn die Größe der zu importierenden Datei 10 MB überschreitet, wird eine Fehlermeldung angezeigt und der Importvorgang wird zurückgewiesen.

Das Skript wird in der Datenbank gespeichert.

34.5.2 Bearbeiten von Skripten

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** mit einer Übersicht über die geplanten Tasks wird angezeigt.

2. Wählen Sie den gewünschten Task und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Der **<Task-Name> Eigenschaften** Dialog mit den Eigenschaften des ausgewählten Tasks wird angezeigt.

3. Klicken Sie auf die Dropdown-Schaltfläche **Bearbeiten** neben dem Feld **Skript**.

   Die Dropdownliste zeigt alle Editor-Programme, die für die Bearbeitung des Skripts zur Verfügung stehen.

4. Wählen Sie den Editor, den Sie verwenden möchten.

   Das Skript wird im ausgewählten Editor geöffnet.

5. Nehmen Sie Ihre Änderungen vor und speichern Sie sie.

   Der Editor wird geschlossen und der Dialog **<Task-Name> Eigenschaften** wird wieder angezeigt.

6. Klicken Sie auf **OK**.

Das geänderte Skript wird in der Datenbank gespeichert.

34.5.3 Export von Skripts

1. Wählen Sie in der SafeGuard Management Center Menüleiste **Extras > Taskplaner**.

   Der Dialog **Taskplaner** mit einer Übersicht über die geplanten Tasks wird angezeigt.

2. Wählen Sie den gewünschten Task und klicken Sie auf die Schaltfläche **Eigenschaften**.

   Der **<Task-Name> Eigenschaften** Dialog mit den Eigenschaften des ausgewählten Tasks wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Exportieren...** neben dem Feld **Skript**.

   Ein **Speichern unter** Dialog wird angezeigt.

4. Wählen Sie den Speicherort zum Speichern des Skripts ein und klicken Sie auf **Speichern**.

   Das Skript wird am angegebenen Speicherort gespeichert.

34.5.4 Vordefinierte Skripte für periodische Tasks

In SafeGuard Enterprise stehen folgende vordefinierte Skripte zur Verfügung:

- ActiveDirectorySynchronization.vbs

  Verwenden Sie dieses Skript für die automatische Synchronisierung zwischen dem Active Directory und SafeGuard Enterprise.

- EventLogDeletion.vbs

  Verwenden Sie dieses Skript, um protokollierte Ereignisse automatisch zu löschen.

Die Skripte werden automatisch im Unterverzeichnis Script Templates der SafeGuard Management Center Installation installiert.

Um diese Skripte für Tasks zu verwenden, importieren Sie sie in den **Taskplaner** und nehmen Sie vor der Anwendung die notwendigen Parameteränderungen vor.

34.5.4.1 Vordefiniertes Skript für die Active Directory Synchronisierung

Sie haben die Möglichkeit, eine bestehende Organisationsstruktur über ein Active Directory in die SafeGuard Enterprise Datenbank zu importieren. Weitere Informationen finden Sie unter Importieren der Organisationsstruktur (Seite 43).

Nach dem Importieren der Struktur können Sie einen periodischen Task für die automatische Synchronisierung zwischen dem Active Directory und SafeGuard Enterprise erstellen. Für diesen Task können Sie das vordefinierte Skript ActiveDirectorySynchronization.vbs verwenden.

Das Skript synchronisiert alle vorhandenen Container in der SafeGuard Enterprise Datenbank mit einem Active Directory.

Bevor Sie das Skript in einem periodischen Task verwenden, können Sie folgende Parameter anpassen:

Parameter	Beschreibung
`logFileName`	Legen Sie den Ausgabepfad für die Skript-Protokolldatei fest. Dieser Parameter ist obligatorisch. Ist der Parameter leer oder ungültig, so kann die Synchronisierung nicht durchgeführt werden und es wird eine Fehlermeldung angezeigt. Standardmäßig ist dieser Parameter leer. Ist bereits eine Protokolldatei vorhanden, so werden neue Protokolle am Ende der Datei angehängt.
`synchronizeMembership`	Setzen Sie diesen Parameter auf 1, um auch Mitgliedschaften zu synchronisieren. Wenn dieser Parameter auf 0 gesetzt ist, werden die Mitgliedschaften nicht synchronisiert. Die Standardeinstellung ist 1.
`synchronizeAccountState`	Setzen Sie diesen Parameter auf 1, um auch den Benutzer Aktiv-Status zu synchronisieren. Wenn dieser Parameter auf 0 gesetzt ist, wird der Benutzer Aktiv-Status nicht synchronisiert. Die Standardeinstellung ist 0.

Hinweis: Stellen Sie sicher, dass sie über die erforderlichen Zugriffsrechte für die Active Directory Synchronisierung verfügen und dass die notwendigen SQL Berechtigungen für das Konto, das für die Ausführung des SafeGuard Enterprise **Taskplaners** benutzt wird, eingestellt sind. Weitere Informationen finden Sie unter Zugriffsrechte für Sicherheitsbeauftragte und Import aus Active Directory (Seite 45). Für Informationen zum Einstellen der Active Directory Zugriffsrechte, siehe http://www.sophos.com/support/knowledgebase/107979.aspx. Für Informationen zum Einstellen der SQL-Berechtigungen, siehe http://www.sophos.com/de-de/support/knowledgebase/113582.aspx.

Wenn die Rechte korrekt eingestellt sind, wenden Sie die Änderungen an und starten Sie den Dienst neu. Wechseln Sie auf den Server, der die SafeGuard Web-Seite hostet. Klicken Sie **Start > Run > Services.msc**, um die **Services** Oberfläche zu öffnen. Klicken Sie mit der rechten Maustaste auf **SafeGuard® Scheduler Service** und klicken Sie auf **All Tasks** > **Restart**.

Hinweis: Wir empfehlen, dass Sie das Active Directory in einem vergleichsweise moderaten Abstand (maximal zweimal am Tag) synchronisieren, damit sich die Serverleistung nicht bedeutend verringert. Neue Objekte werden in diesen Abständen im SafeGuard Management Center unter .Autoregistered angezeigt. Hier können Sie wie üblich verwaltet werden.

34.5.4.2 Vordefiniertes Skript für das automatische Löschen von protokollierten Ereignissen

Die in der SafeGuard Enterprise Datenbank protokollierten Ereignisse werden in der EVENT-Tabelle gespeichert. Weitere Informationen zur Protokollierung finden Sie unter Berichte (Seite 270).

Mit dem **Taskplaner** können Sie einen periodischen Task für das automatische Löschen von protokollierten Ereignissen erstellen. Für diesen Task können Sie das vordefinierte Skript EventLogDeletion.vbs verwenden.

Das Skript löscht Ereignisse aus der EVENT-Tabelle. Wenn Sie den entsprechenden Parameter einstellen, verschiebt das Skript auch die Ereignisse aus der EVENT-Tabelle in die Backup-Log-Tabelle EVENT_BACKUP. Dabei wird eine definierte Anzahl an neuesten Ereignissen in der EVENT-Tabelle belassen.

Bevor Sie das Skript in einem periodischen Task verwenden, können Sie folgende Parameter anpassen:

Parameter	Beschreibung
`maxDuration`	Mit diesem Parameter legen Sie fest, wie lange (in Tagen) die Ereignisse in der EVENT-Tabelle verbleiben. Die Standardeinstellung ist 0. Wenn dieser Parameter auf 0 gesetzt ist, gibt es keine zeitliche Begrenzung für das Verbleiben der Ereignisse in der EVENT-Tabelle.
`maxCount`	Mit diesem Parameter legen Sie fest, wie viele Ereignisse in der EVENT-Tabelle verbleiben. Die Standardeinstellung ist 5000. Wenn dieser Parameter auf 0 gesetzt ist, gibt es keine maximale Anzahl an Ereignissen in der EVENT-Tabelle.
`keepBackup`	Mit diesem Parameter legen Sie fest, ob Ereignisse in der EVENT_BACKUP-Tabelle gesichert werden sollen. Die Standardeinstellung ist 0. Wenn dieser Parameter auf 0 gesetzt ist, werden die Ereignisse nicht gesichert. Setzen Sie diesen Parameter auf 1, um eine Sicherungskopie der gelöschten Ereignisse zu erstellen.

Hinweis: Wenn Sie die Ereignisse über das Skript aus der EVENT-Tabelle in die Backup-Log-Tabelle verschieben, findet die Verkettung der Protokollierung keine Anwendung mehr. Es ist nicht sinnvoll, die Verkettung zu aktivieren und gleichzeitig die gespeicherte Prozedur zur Säuberung der EVENT-Tabelle einzusetzen. Weitere Informationen finden Sie unter Verkettung von protokollierten Ereignissen (Seite 277).

34.6 Einschränkungen in Bezug auf registrierte Server

Wenn Sie im SafeGuard Management Center mit der Funktion **Konfigurationspakete** Server registrieren, können Sie mit einem Maschinenzertifikat mehrere Server Templates registrieren. Sie können jedoch jeweils nur ein Template auf der realen Maschine installieren.

Wenn Sie für beide Server das Kontrollkästchen **Skripts ausführen erlaubt** auswählen, zeigt der **Taskplaner** beide Server in der Dropdownliste **SGN Server** in den Dialogen **Neuer Task** und **<Task-Name> Eigenschaften** zur Auswahl an. Der **Taskplaner** kann nicht ermitteln, welches der beiden Templates auf der Maschine installiert wurde.

Um dies zu vermeiden, wählen Sie das Kontrollkästchen **Skript ausführen erlaubt** für Templates, die nicht auf dem Server installiert sind, nicht aus. Vermeiden Sie außerdem eine Doppelung von Templates mit demselben Maschinenzertifikat.

Weitere Informationen zum Registrieren von Servern finden Sie in der *SafeGuard Enterprise Installationsanleitung*.

34.7 Protokollierte Ereignisse für den Taskplaner

Zur Ausführung von Tasks lassen sich Ereignisse protokollieren, die zum Beispiel bei der Fehlerbehebung nützliche Informationen liefern. Sie können festlegen, dass folgende Ereignisse protokolliert werden:

- Task erfolgreich ausgeführt
- Task fehlgeschlagen
- Service Thread wegen Ausführung gestoppt

Die Ereignisse enthalten den Output der Skriptkonsole zur Unterstützung bei der Fehlerbehebung.

Weitere Informationen zur Protokollierung finden Sie unter Berichte (Seite 270).

35 Managing Mac endpoints in the SafeGuard Management Center

Macs, auf denen die folgenden Sophos Produkte installiert sind, können von SafeGuard Enterprise verwaltet werden und/oder Statusinformationen melden. Die Statusinformationen werden im SafeGuard Management Center angezeigt:

- Sophos SafeGuard File Encryption für Mac 6.1 und höher
- Sophos SafeGuard Disk Encryption für Mac 6.1/Sophos SafeGuard Native Device Encryption 7.0
- Sophos SafeGuard Disk Encryption for Mac 6 - nur Berichte

Hinweis:

Empfehlungen, Besonderheiten und Beschränkungen bei der Verwendung von SafeGuard File Encryption oder Disk/Native Device Encryption für Mac finden Sie in der Administratorhilfe dieser Produkte.

35.1 Bestands- und Statusinformationen für Macs

Für Macs liefert der **Bestand** u. a. folgende Informationen zu den einzelnen Maschinen: Die angezeigten Daten können variieren, je nachdem, welches Sophos Produkt installiert ist:

- Name des Mac
- Betriebssystem
- POA-Typ
- POA-Status
- Anzahl an verschlüsselten Laufwerken
- Anzahl an unverschlüsselten Laufwerken
- Letzter Server-Kontakt
- Änderungsdatum
- Informationen dazu, ob das aktuelle Unternehmenszertifikat verwendet wird.

35.2 Erzeugen eines Konfigurationspakets für Macs

Ein Konfigurationspaket für einen Mac enthält die relevanten Serverinformationen sowie das Unternehmenszertifikat. Der Mac benutzt diese Informationen zum Zurückmelden von

Statusinformationen (SafeGuard POA an/aus, Verschlüsselungsstatus usw.). Die Statusinformationen werden im SafeGuard Management Center angezeigt.

1. Klicken Sie im SafeGuard Management Center im **Extras** Menü auf **Konfigurationspakete**.
2. Wählen Sie **Pakete für Managed Clients**.
3. Klicken Sie auf **Konfigurationspaket hinzufügen**.
4. Geben Sie einen beliebigen Namen für das Konfigurationspaket ein.
5. Ordnen Sie einen primären SafeGuard Enterprise Server zu (der sekundäre Server ist nicht notwendig).
6. Wählen Sie **SSL** als **Transportverschlüsselung** für die Verbindung zwischen dem Endpoint und dem SafeGuard Enterprise Server. Für Macs wird **Sophos** als **Transportverschlüsselung** nicht unterstützt.
7. Geben Sie einen Ausgabepfad für das Konfigurationspaket (ZIP) an.
8. Klicken Sie auf **Konfigurationspaket erstellen**.

   Die Server-Verbindung für den SSL **Transportverschlüsselung** Modus wird validiert. Wenn die Verbindung fehlschlägt, wird eine Warnungsmeldung angezeigt.

Das Konfigurationspaket (ZIP) wird nun im angegebenen Verzeichnis angelegt. Sie müssen das Paket auf Ihren Macs verteilen und installieren.

36 SafeGuard Enterprise und selbst-verschlüsselnde Opal-Festplatten

Selbst-verschlüsselnde Festplatten bieten hardware-basierende Verschlüsselung der Daten, die auf die Festplatte geschrieben werden. Die Trusted Computing Group (TCG) hat den anbieter-unabhängigen Opal-Standard für selbst-verschlüsselnde Festplatten veröffentlicht. Festplatten, die dem Opal-Standard entsprechen, werden von unterschiedlichen Herstellern angeboten. SafeGuard Enterprise unterstützt den Opal-Standard und bietet die Verwaltung von Endpoints mit selbst-verschlüsselnden Festplatten, die dem Opal-Standard entsprechen. Siehe auch http://www.sophos.com/de-de/support/knowledgebase/113366.aspx.

36.1 Integration von Opal-Festplatten in SafeGuard Enterprise

In SafeGuard Enterprise lassen sich Endpoints mit selbst-verschlüsselnden Opal-Festplatten wie alle anderen durch SafeGuard Enterprise geschützten Endpoints über das SafeGuard Management Center verwalten.

Die zentrale und vollständig transparente Verwaltung von Opal-Festplatten durch SafeGuard Enterprise ermöglicht somit die Anwendung in heterogenen IT-Umgebungen. Durch die Unterstützung des Opal-Standards bieten wir den vollen Funktionsumfang von SafeGuard Enterprise für Benutzer von selbst-verschlüsselnden Opal-Festplatten. In Verbindung mit SafeGuard Enterprise bieten Opal-Festplatten erweiterte Sicherheits-Featrures.

36.2 Aufwertung von Opal-Festplatten mit SafeGuard Enterprise

Die Verwaltung von selbst-verschlüsselnden Opal-Festplatten mit SafeGuard Enterprise bietet Ihnen folgende Vorteile:

- Zentrale Verwaltung der Endpoints
- SafeGuard Power-on Authentication mit grafischer Benutzeroberfläche
- Unterstützung mehrerer Benutzer
- Unterstützung der Anmeldung mit Token/Smartcard
- Unterstützung der Anmeldung mit Fingerabdruck
- Recovery (Local Self Help, Challenge/Response)
- Zentral verwaltete Protokollierung
- Verschlüsselung von Wechselmedien (z. B. USB-Sticks) mit SafeGuard Data Exchange

36.3 Verwaltung von Endpoints mit Opal-Festplatten durch SafeGuard Enterprise

Sie können Endpoints mit selbst-verschlüsselnden Opal-Festplatten im SafeGuard Management Center wie alle anderen durch SafeGuard Enterprise geschützten Endpoints verwalten. Als Sicherheitsbeauftragter können Sie Sicherheitsrichtlinien (z. B. für die Authentisierung) erstellen und sie an die Endpoints verteilen.

Sobald ein Endpoint mit einer Opal-Festplatte bei SafeGuard Enterprise registriert ist, werden Informationen zu Benutzer, Computer, Anmeldemodus und Verschlüsselungsstatus angezeigt. Außerdem werden Ereignisse protokolliert.

Die Verwaltung von Endpoints mit Opal-Festplatten in SafeGuard Enterprise ist transparent. Das heißt, die Verwaltungsfunktionen haben im Allgemeinen dieselbe Funktionsweise wie für andere durch SafeGuard Enterprise geschützte Endpoints. Der Computertyp lässt sich in der Registerkarte **Bestand** eines Containers unter **Benutzer & Computer** ermitteln. Die Spalte **POA-Typ** zeigt an, ob der betreffende Computer durch SafeGuard Enterprise verschlüsselt ist oder eine selbst-verschlüsselnde Opal-Festplatte verwendet.

36.4 Verschlüsselung von Opal-Festplatten

Festplatten, die dem Opal-Standard entsprechen, sind selbst-verschlüsselnd. Daten werden automatisch verschlüsselt, wenn sie auf die Festplatte geschrieben werden.

Die Festplatten werden mit einem AES 128/256 Schlüssel als Opal-Kennwort gesperrt. Dieses Kennwort wird von SafeGuard Enterprise über eine Verschlüsselungsrichtlinie verwaltet (siehe Sperren von Opal-Festplatten (Seite 296)).

36.5 Sperren von Opal-Festplatten

Um Opal-Festplatten zu sperren, muss für mindestens ein Volume auf der Festplatte der Computerschlüssel in einer Verschlüsselungsrichtlinie definiert werden. Wenn die Verschlüsselungsrichtlinie ein Boot-Volume umfasst, wird der Computerschlüssel automatisch definiert.

1. Erstellen Sie im SafeGuard Management Center eine Richtlinie vom Typ **Geräteschutz**.
2. Wählen Sie im **Verschlüsselungsmodus für Medien** Feld die Einstellung **Volume-basierend**.
3. Wählen Sie im Feld **Schlüssel für die Verschlüsselung** die Einstellung **Definierter Computerschlüssel**.
4. Speichern Sie Ihre Änderungen in der Datenbank.
5. Übertragen Sie die Richtlinie an den relevanten Endpoint.

Die Opal-Festplatte ist gesperrt. Der Zugriff ist nur über die Anmeldung an der SafeGuard Power-on Authentication möglich.

36.6 Berechtigung von Benutzern zum Entsperren von Opal-Festplatten

Als Sicherheitsbeauftragter können Sie Benutzer dazu berechtigen, Opal-Festplatten auf ihren Endpoints mit dem **Entschlüsseln** Befehl aus dem Windows Explorer Kontextmenü zu entsperren.

Voraussetzung: In der Geräteschutz-Richtlinie, die für die Opal-Festplatte gilt, muss die Option **Benutzer darf Volume entschlüsseln** auf **Ja** eingestellt sein.

1. Erstellen Sie im SafeGuard Management Center eine Richtlinie vom Typ **Geräteschutz** und beziehen Sie alle Volumes auf der Opal-Festplatte in die Richtlinie ein.
2. Wählen Sie im **Verschlüsselungsmodus für Medien** Feld die Einstellung **Keine Verschlüsselung**.
3. Speichern Sie Ihre Änderungen in der Datenbank.
4. Übertragen Sie die Richtlinie an den relevanten Endpoint.

Der Benutzer kann die Opal-Festplatte auf dem Endpoint entsperren. In der Zwischenzeit bleibt die Festplatte gesperrt.

36.7 Protokollierung von Ereignissen für Endpoints mit Opal-Festplatten

Von Endpoints mit selbst-verschlüsselnden Opal-Festplatten gemeldete Ereignisse werden wie für alle anderen durch SafeGuard Enterprise geschützten Endpoints protokolliert. Dabei wird der Computertyp nicht explizit erwähnt. Die gemeldeten Ereignisse entsprechen den von alle anderen durch SafeGuard Enterprise geschützten Endpoints gemeldeten Ereignisse.

Weitere Informationen finden Sie unter Berichte (Seite 270).

37 Für Berichte auswählbare Ereignisse

Die folgende Tabelle bietet einen Überblick zu allen für die Protokollierung auswählbaren Ereignissen.

Kategorie	Ereignis-ID	Beschreibung
System	1005	Dienst gestartet.
System	1006	Dienst starten fehlgeschlagen
System	1007	Dienst angehalten.
System	1016	Integritätstest der Dateien fehlgeschlagen.
System	1017	Logging Ziel nicht verfügbar.
System	1018	Nicht genehmigter Versuch SafeGuard Enterprise zu deinstallieren
Authentisierung	2001	Externe GINA erkannt und erfolgreich eingebunden.
Authentisierung	2002	Externe GINA erkannt, Einbindung fehlgeschlagen.
Authentisierung	2003	Power-on Authentication ist aktiviert.
Authentisierung	2004	Power-on Authentication ist deaktiviert.
Authentisierung	2005	Wake on LAN ist aktiviert.
Authentisierung	2006	Wake on LAN ist deaktiviert.
Authentisierung	2007	Challenge erzeugt.
Authentisierung	2008	Response erzeugt.
Authentisierung	2009	Anmeldung erfolgreich durchgeführt.
Authentisierung	2010	Anmeldung fehlgeschlagen.
Authentisierung	2011	Benutzer während Anmeldung importiert und als Besitzer markiert.
Authentisierung	2012	Benutzer vom Besitzer importiert und als Nicht- Besitzer markiert
Authentisierung	2013	Benutzer von Nicht-Besitzer importiert und als Nicht-Besitzer markiert.
Authentisierung	2014	Benutzer als Besitzer entfernt.

Kategorie	Ereignis-ID	Beschreibung
Authentisierung	2015	Import des Benutzers während der Anmeldung fehlgeschlagen.
Authentisierung	2016	Benutzer hat sich abgemeldet.
Authentisierung	2017	Benutzer wurde zwangsweise abgemeldet.
Authentisierung	2018	Aktion wurde auf dem Gerät ausgeführt.
Authentisierung	2019	Benutzer hat einen Kennwort/PIN-Wechsel eingeleitet.
Authentisierung	2020	Der Benutzer hat nach der Anmeldung sein Kennwort/PIN geändert.
Authentisierung	2021	Kennwort/PIN-Qualität.
Authentisierung	2022	Verstoß gegen Kennwort-/PIN-Richtlinie.
Authentisierung	2023	Der LocalCache war beschädigte und wurde restauriert
Authentisierung	2024	Ungültige Passwort Blacklist Konfiguration
Authentisierung	2025	Der empfangene Response Code erlaubt es dem Benutzer, sich sein Passwort anzeigen zu lassen.
Authentisierung	2030	Angemeldeter Benutzer ist Service Account.
Authentisierung	2035	Anmeldung
Authentisierung	2036	Service Account Liste gelöscht.
Authentisierung	2056	SGN Windows-Benutzer hinzufügen
Authentisierung	2057	SGN Windows-Benutzer von der Maschine entfernen.
Authentisierung	2058	Entfernen des UMA-Benutzers
Authentisierung	2061	Rückgabewert der Computrace-Überprüfung.
Authentisierung	2062	Computrace-Überprüfung konnte nicht ausgeführt werden.
Authentisierung	2071	Kernelinitialisierung erfolgreich abgeschlossen.
Authentisierung	2071	Kernel-Initialisierung ist fehlgeschlagen.
Authentisierung	2073	Maschinenschlüssel wurden auf dem Client erfolgreich erzeugt.
Authentisierung	2074	Maschinenschlüssel konnten auf dem Client nicht erzeugt werden. Interner Code: 0x%1.

Kategorie	Ereignis-ID	Beschreibung
Authentisierung	2075	Abfrage der Platteneigenschaften oder Opal-Initialisierung ist fehlgeschlagen. Interner Code: 0x%1.
Authentisierung	2079	Importieren eines Benutzers in den Kernel wurde erfolgreich beendet.
Authentisierung	2080	Löschen eines Benutzers aus dem Kernel wurde erfolgreich beendet.
Authentisierung	2081	Import eines Benutzers in den Kernel ist fehlgeschlagen.
Authentisierung	2082	Löschen eines Benutzers aus dem Kernel ist fehlgeschlagen.
Authentisierung	2083	Response mit Aktion "Benutzer wird sein Kennwort angezeigt" erzeugt.
Authentisierung	2084	Response für virtuellen Client erzeugt.
Authentisierung	2085	Response für Standalone Client erzeugt.
Authentisierung	2095	Wake on LAN konnte nicht aktiviert werden.
Authentisierung		Ein Zertifkat wurde einem Standalone-Client-Benutzer zugewiesen.
Authentisierung	2096	Wake on LAN konnte nicht deaktiviert werden.
Authentisierung	2097	Der Benutzer hat sich zum ersten Mal mit dem Standby-Token am Client angemeldet. Der Standby-Token wurde als Standard-Token eingestellt.
Authentisierung	2098	Die erfolgreiche Aktivierung eines Standby-Certificate wurde dem Server gemeldet.
Authentisierung	2099	Der Benutzer hat sich zum ersten Mal mit dem Standby-Token am Client angemeldet. Das Standby-Zertifikate konnte aufgrund eines Fehlers nicht aktiviert werden.
Authentisierung	2100	Die Aktivierung eines Standby-Certificate ist auf dem Server fehlgeschlagen.
Administration	2500	SafeGuard Enterprise Administration gestartet.
Administration	2501	Anmeldung an der SafeGuard Enterprise Administration fehlgeschlagen
Administration	2502	Autorisierung an der SafeGuard Enterprise Administration fehlgeschlagen.
Administration	2504	Benutzer genehmigt zusätzliche Autorisierung

Kategorie	Ereignis-ID	Beschreibung
Administration	2505	Zusätzliche Autorisierung von Benutzer fehlgeschlagen.
Administration	2506	Datenimport vom Verzeichnis erfolgreich.
Administration	2507	Datenimport vom Verzeichnis abgebrochen.
Administration	2508	Datenimport vom Verzeichnis fehlgeschlagen.
Administration	2511	Benutzer angelegt.
Administration	2513	Benutzer wurde geändert.
Administration	2515	Benutzer gelöscht.
Administration	2518	Anlegen des Benutzers fehlgeschlagen.
Administration	2522	Löschen des Benutzers fehlgeschlagen.
Administration	2525	Computer angelegt
Administration	2529	Computer gelöscht.
Administration	2532	Anlegen des Computers fehlgeschlagen.
Administration	2536	Löschen des Computers fehlgeschlagen.
Administration	2539	OU angelegt.
Administration	2543	OU gelöscht.
Administration	2546	Anlegen der OU fehlgeschlagen
Administration	2547	Importieren der OU fehlgeschlagen.
Administration	2550	Löschen der OU fehlgeschlagen.
Administration	2553	Gruppe angelegt.
Administration	2555	Gruppe geändert.
Administration	2556	Gruppe umbenannt.
Administration	2557	Gruppe gelöscht.
Administration	2560	Anlegen der Gruppe fehlgeschlagen.
Administration	2562	Ändern der Gruppe fehlgeschlagen.
Administration	2563	Umbenennen der Gruppe fehlgeschlagen.

Kategorie	Ereignis-ID	Beschreibung
Administration	2564	Löschen der Gruppe fehlgeschlagen.
Administration	2573	Mitglieder der Gruppe hinzugefügt.
Administration	2575	Mitglieder aus Gruppe entfernt.
Administration	2576	Hinzufügen der Mitglieder zur Gruppe fehlgeschlagen.
Administration	2578	Entfernen der Mitglieder aus Gruppe fehlgeschlagen.
Administration	2580	Gruppe von OU nach OU verschoben.
Administration	2583	Verschieben der Gruppe von OU nach OU fehlgeschlagen.
Administration	2591	Objekte der Gruppe hinzugefügt.
Administration	2593	Objekte aus Gruppe entfernt.
Administration	2594	Hinzufügen der Objekte zur Gruppe fehlgeschlagen
Administration	2596	Hinzufügen der Objekte aus Gruppe fehlgeschlagen
Administration	2603	Schlüssel erzeugt. Algorithmus.
Administration	2607	Schlüssel zugeordnet.
Administration	2608	Schlüsselzuordnung aufgehoben.
Administration	2609	Erzeugen des Schlüssels fehlgeschlagen.
Administration	2613	Zuordnung des Schlüssels fehlgeschlagen.
Administration	2614	Entfernen der Zuordnung des Schlüssels fehlgeschlagen.
Administration	2615	Zertifikat erzeugt.
Administration	2616	Zertifikat importiert.
Administration	2619	Zertifikat gelöscht.
Administration	2621	Zertifikat Benutzer zugeordnet.
Administration	2622	Zertifikatszuordnung zu Benutzer aufgehoben.
Administration	2623	Erzeugen des Zertifikats fehlgeschlagen.
Administration	2624	Importieren des Zertifikats fehlgeschlagen.
Administration	2627	Löschen des Zertifikats fehlgeschlagen.

Kategorie	Ereignis-ID	Beschreibung
Administration	2628	Verlängern des Zertifikats fehlgeschlagen.
Administration	2629	Zuordnen des Zertifikats zu Benutzer fehlgeschlagen.
Administration	2630	Entfernen der Zuordnung des Zertifikats vom Benutzer fehlgeschlagen.
Administration	2631	Token eingesteckt.
Administration	2632	Token entfernt.
Administration	2633	Token wurde für Benutzer ausgestellt.
Administration	2634	PIN des Benutzers auf Token ändern.
Administration	2635	PIN des Sicherheitsbeauftragten auf Token ändern.
Administration	2636	Token wurde gesperrt.
Administration	2637	Token entsperrt.
Administration	2638	Token gelöscht.
Administration	2639	Tokenzuordnung für Benutzer aufgehoben.
Administration	2640	Ausstellen des Tokens für Benutzer fehlgeschlagen.
Administration	2641	Ändern der Benutzer-PIN auf Token fehlgeschlagen.
Administration	2642	Ändern der Sicherheitsbeauftragten-PIN auf Token fehlgeschlagen.
Administration	2643	Sperren des Tokens fehlgeschlagen.
Administration	2644	Entsperren des Tokens fehlgeschlagen.
Administration	2645	Löschen des Tokens fehlgeschlagen.
Administration	2647	Richtlinie erstellt.
Administration	2648	Richtlinie geändert.
Administration	2650	Richtlinie gelöscht.
Administration	2651	Richtlinie der OU zugewiesen und aktiviert.
Administration	2652	Zugewiesene Richtlinie wurde von OU entfernt.
Administration	2653	Erstellen der Richtlinie fehlgeschlagen.

Kategorie	Ereignis-ID	Beschreibung
Administration	2654	Ändern der Richtlinie fehlgeschlagen.
Administration	2657	Zuweisung und Aktivierung der Richtlinie zu OU fehlgeschlagen.
Administration	2658	Entfernen der zugewiesenen Richtlinie von OU ist fehlgeschlagen.
Administration	2659	Richtlinien-Gruppe angelegt.
Administration	2660	Richtlinien-Gruppe geändert.
Administration	2661	Richtlinien-Gruppe gelöscht.
Administration	2662	Anlegen der Richtlinien-Gruppe fehlgeschlagen.
Administration	2663	Ändern der Richtlinien-Gruppe fehlgeschlagen.
Administration	2665	Folgende Richtlinie wurde der Richtlinien-Gruppe hinzugefügt.
Administration	2667	Folgende Richtlinie wurde aus der Richtlinien-Gruppe entfernt.
Administration	2668	Hinzufügen der Richtlinie zur Richtlinien-Gruppe fehlgeschlagen.
Administration	2670	Entfernen der Richtlinie aus Richtlinien-Gruppe fehlgeschlagen.
Administration	2678	Protokollierte Ereignisse exportiert.
Administration	2679	Exportieren der protokollierten Ereignisse fehlgeschlagen.
Administration	2680	Protokollierte Ereignisse gelöscht.
Administration	2681	Löschen der protokollierten Ereignisse fehlgeschlagen.
Administration	2684	Sicherheitsbeauftragter erlaubt die Erneuerung eines Zertifikats
Administration	2685	Beauftragter verbietet die Erneuerung eines Zertifikats
Administration	2686	Änderungen an den Einstellungen für die Zertifikatserneuerung fehlgeschlagen
Administration	2687	Zertifikat für Beauftragten gewechselt
Administration	2688	Zertifikatswechsel für Beauftragten fehlgeschlagen
Administration	2692	Erzeugen von Arbeitsgruppen.
Administration	2693	Fehlgeschlagenes Erzeugen von Arbeitsgruppen
Administration	2694	Löschen von Arbeitsgruppen.

Kategorie	Ereignis-ID	Beschreibung
Administration	2695	Fehlgeschlagenes Löschen von Arbeitsgruppen
Administration	2696	Erzeugen von Benutzern.
Administration	2697	Fehlgeschlagenes Erzeugen von Benutzern.
Administration	2698	Erzeugen von Maschinen.
Administration	2699	Fehlgeschlagenes Erzeugen von Maschinen.
Administration	2700	Die Lizenz wurde verletzt.
Administration	2701	Schlüsseldatei wurde erzeugt.
Administration	2702	Schlüssel für Schlüsseldatei wurde gelöscht.
Administration	2703	Sicherheitsbeauftragter hat die Power-on Authentication in einer Richtlinie deaktiviert.
Administration	2704	LSH Fragenthema erstellt.
Administration	2705	LSH Fragenthema geändert.
Administration	2706	LSH Fragenthema gelöscht.
Administration	2707	Frage geändert.
Administration	2753	Schreibgeschützt-Zugriff auf den Container '%1' wurde dem Sicherheitsbeauftragten '%2' zugeordnet.
Administration	2755	Voller Zugriff auf Container '%1' wurde dem Sicherheitsbeauftragten '%2' zugeordnet.
Administration	2757	Zugriff auf Container '%1' wurde dem Sicherheitsbeauftragten '%2' entzogen.
Administration	2766	Zugriff auf Container '%1' wurde für den Sicherheitsbeauftragten '%2' explizit verweigert.
Administration	2767	Verweigerter Zugriff auf Container '%1' wurde für Sicherheitsbeauftragten '%2' widerrufen.
Administration	2768	Lesezugriff auf Container '%1' wurde dem Sicherheitsbeauftragten '%2' zugeordnet.
Administration	2810	POA-Benutzer %1 angelegt.
Administration	2811	POA-Benutzer %1 geändert.
Administration	2812	POA-Benutzer %1 gelöscht.

Kategorie	Ereignis-ID	Beschreibung
Administration	2815	Erstellen von POA-Benutzer "%1" fehlgeschlagen.
Administration	2816	Ändern von POA-Benutzer "%1" fehlgeschlagen.
Administration	2817	Löschen von POA-Benutzer "%1" fehlgeschlagen.
Administration	2820	POA-Gruppe %1 angelegt.
Administration	2821	POA-Gruppe %1 geändert.
Administration	2822	POA-Gruppe %1 gelöscht.
Administration	2825	Erstellen von POA-Gruppe "%1" fehlgeschlagen.
Administration	2826	Ändern von POA-Gruppe "%1" fehlgeschlagen.
Administration	2827	Löschen von POA-Gruppe "%1" fehlgeschlagen.
Administration	2850	Taskplaner-Dienst wurde wegen eines Ausnahmefehlers angehalten.
Administration	2851	Task-Planer Task erfolgreich ausgeführt
Administration	2852	Task-Planer Task fehlgeschlagen
Administration	2853	Task-Planer Task erzeugt oder geändert
Administration	2854	Task-Planer Task gelöscht
Client	3003	Kernelsicherung erfolgreich
Client	3005	Kernelrücksicherung beim ersten Versuch erfolgreich
Client	3006	Kernelrücksicherung beim zweiten Versuch erfolgreich
Client	3007	Kernelsicherung fehlgeschlagen
Client	3008	Kernelrücksicherung fehlgeschlagen
Client	3020	Datei-Tracking für Wechselmedien: Eine Datei wurde erstellt.
Client	3021	Datei-Tracking für Wechselmedien: Eine Datei wurde umbenannt.
Client	3022	Datei-Tracking für Wechselmedien: Eine Datei wurde gelöscht.
Client	3025	Datei-Tracking für Cloud-Speicher: Eine Datei wurde erstellt.
Client	3026	Datei-Tracking für Cloud-Speicher: Eine Datei wurde umbenannt.

Kategorie	Ereignis-ID	Beschreibung
Client	3027	Datei-Tracking für Cloud-Speicher: Eine Datei wurde gelöscht.
Client	3030	Benutzer hat LSH-Informationen nach Anmeldung geändert.
Client	3035	LSH aktiviert.
Client	3040	LSH deaktiviert.
Client	3045	LSH verfügbar - Enterprise Client
Client	3046	LSH verfügbar - Standalone Client
Client	3050	LSH deaktiviert - Enterprise Client
Client	3051	LSH nicht verfügbar - Standalone Client
Client	3055	QST Liste (LSH Fragen) geändert.
Client	3405	Deinstallation des Configuration Protection Clients fehlgeschlagen.
Client	3070	Schlüssel-Backup auf Netzwerkfreigabe gespeichert.
Client	3071	Schlüssel-Backup konnte nicht auf der angegebenen Netzwerkfreigabe gespeichert werden.
Client	3110	POA-Benutzer "%1" in POA importiert.
Client	3111	POA-Benutzer "%1" aus POA gelöscht.
Client	3115	POA -Benutzer "%1": Kennwort mit F8 geändert.
Client	3116	Import von POA-Benutzer "%1" in POA fehlgeschlagen.
Client	3117	Löschen von POA-Benutzer "%1" aus POA fehlgeschlagen.
Client	3118	POA-Benutzer "%1": Kennwortänderung mit F8 fehlgeschlagen.
Client	3406	Interner Fehler im Configuration Protection Client
Client	3407	Mögliche Ereignis-Manipulation im Configuration Protection Client
Client	3408	Mögliche Ereignisprotokoll-Manipulation im Configuration Protection Client
Verschlüsselung	3501	Zugriff auf Medium auf Laufwerk verweigert.
Verschlüsselung	3502	Zugriff auf Datendatei verweigert.
Verschlüsselung	3503	Sektorbasierte Erst-Verschlüsselung des Laufwerks gestartet.

Kategorie	Ereignis-ID	Beschreibung
Verschlüsselung	3504	Sektorbasierte Erst-Verschlüsselung des Laufwerks gestartet. (Schnellmodus)
Verschlüsselung	3505	Sektorbasierte Erst-Verschlüsselung des Laufwerks fehlerfrei beendet.
Verschlüsselung	3506	Sektorbasierte Erst-Verschlüsselung des Laufwerks gescheitert und beendet.
Verschlüsselung	3507	Sektorbasierte Erst-Verschlüsselung des Laufwerks abgebrochen.
Verschlüsselung	3508	Sektorbasierte Erst-Verschlüsselung des Laufwerks fehlgeschlagen.
Verschlüsselung	3509	Sektorbasierte Entschlüsselung des Laufwerks gestartet.
Verschlüsselung	3510	Sektorbasierte Entschlüsselung des Laufwerks fehlerfrei beendet.
Verschlüsselung	3511	Sektorbasierte Entschlüsselung des Laufwerks gescheitert und beendet.
Verschlüsselung	3512	Sektorbasierte Entschlüsselung des Laufwerks abgebrochen.
Verschlüsselung	3513	Sektorbasierte Entschlüsselung des Laufwerks fehlgeschlagen.
Verschlüsselung	3514	Dateibasierende Initialverschlüsselung auf einem Laufwerk gestartet.
Verschlüsselung	3515	Dateibasierende Initialverschlüsselung auf einem Laufwerk erfolgreich abgeschlossen.
Verschlüsselung	3516	Dateibasierende Initialverschlüsselung auf einem Laufwerk fehlgeschlagen und beendet.
Verschlüsselung	3517	Dateibasierende Entschlüsselung auf einem Laufwerk abgebrochen.
Verschlüsselung	3519	Dateibasierende Verschlüsselung einer Datei gestartet.
Verschlüsselung	3520	Dateibasierende Verschlüsselung einer Datei erfolgreich abgeschlossen.
Verschlüsselung	3521	Dateibasierende Entschlüsselung auf einem Laufwerk fehlgeschlagen und beendet.
Verschlüsselung	3522	Dateibasierende Entschlüsselung auf einem Laufwerk abgebrochen.
Verschlüsselung	3524	Verschlüsselung einer Datei gestartet.
Verschlüsselung	3525	Verschlüsselung einer Datei erfolgreich abgeschlossen.

Kategorie	Ereignis-ID	Beschreibung
Verschlüsselung	3526	Verschlüsselung einer Datei fehlgeschlagen.
Verschlüsselung	3540	Entschlüsselung einer Datei gestartet.
Verschlüsselung	3541	Entschlüsselung einer Datei erfolgreich abgeschlossen.
Verschlüsselung	3542	Entschlüsselung einer Datei fehlgeschlagen.
Verschlüsselung	3543	Backup von Bootkey durchgeführt
Verschlüsselung	3544	Überschreitung der Anzahl von Verschlüsselungsalgorithmen für Start-Laufwerke
Verschlüsselung	3545	Lesefehler von Schlüsseldatenbereiche
Verschlüsselung	3546	Abweisen von Laufwerken gemäß den Richtlinien.
Verschlüsselung	3547	Warnung NTFS Boot Sector Backup fehlt auf Volume %1.
Verschlüsselung	3548	Der Benutzer hat neue BitLocker-Anmeldeinformationen zum Starten des Computers zur Verfügung gestellt.
Verschlüsselung	3549	Der Benutzer hat versucht, neue BitLocker-Anmeldeinformationen zum Starten des Computers zur Verfügung zu stellen, aber der Vorgang ist fehlgeschlagen.
Verschlüsselung	3560	Zugriffsschutz
Verschlüsselung	3600	Allgemeiner Verschlüsselungsfehler
Verschlüsselung	3601	Verschlüsselungsfehler - Laufwerk nicht gefunden
Verschlüsselung	3602	Verschlüsselungsfehler - Laufwerk nicht verfügbar
Verschlüsselung	3603	Verschlüsselungsfehler - Laufwerk entfernt
Verschlüsselung	3604	Verschlüsselungsfehler - Laufwerksfehler
Verschlüsselung	3607	Verschlüsselungsfehler - Der Schlüssel fehlt
Verschlüsselung	3610	Verschlüsselungsfehler - Der Original-KSA Bereich ist beschädigt.
Verschlüsselung	3611	Verschlüsselungsfehler - Der Sicherungs-KSA Bereich ist beschädigt.
Verschlüsselung	3612	Verschlüsselungsfehler - Der ESA-Bereich ist beschädigt.
Zugriffskontrolle	4400	Port erfolgreich freigegeben
Zugriffskontrolle	4401	Gerät erfolgreich freigegeben

Kategorie	Ereignis-ID	Beschreibung
Zugriffskontrolle	4402	Speichergerät erfolgreich freigegeben
Zugriffskontrolle	4403	WLAN erfolgreich freigegeben
Zugriffskontrolle	4404	Port erfolgreich entfernt
Zugriffskontrolle	4405	Gerät erfolgreich entfernt
Zugriffskontrolle	4406	Speichergerät erfolgreich entfernt
Zugriffskontrolle	4407	WLAN-Verbindung erfolgreich getrennt
Zugriffskontrolle	4408	Port eingeschränkt
Zugriffskontrolle	4409	Gerät eingeschränkt
Zugriffskontrolle	4410	Speichergerät eingeschränkt
Zugriffskontrolle	4411	WLAN eingeschränkt
Zugriffskontrolle	4412	Port gesperrt
Zugriffskontrolle	4413	Gerät gesperrt
Zugriffskontrolle	4414	Speichergerät gesperrt
Zugriffskontrolle	4415	WLAN gesperrt

38 Fehlercodes

38.1 SGMERR-Codes in der Windows-Ereignisanzeige

In der Windows-Ereignisanzeige könnten Sie folgende Meldung finden:

"Authorization for SafeGuard Enterprise Administration failed for user... Grund: SGMERR[536870951]"

Welche Bedeutung die Nummer “536870951” hat, finden Sie in dieser Tabelle. Nummer “536870951” bedeutet zum Beispiel “Die angegebene PIN ist falsch, der Benutzer konnte nicht authentisiert werden".

Fehler-ID	Anzeige
0	OK
21	Interner Fehler entdeckt
22	Modul nicht initialisiert
23	Datei I/O Fehler entdeckt
24	Speicher kann nicht zugewiesen werden
25	Datei I/O Lesefehler
26	Datei I/O Schreibfehler
50	Keine Operation durchgeführt
101	Allgemeiner Fehler
102	Zugriff verweigert
103	Datei existiert bereits
1201	Registry Eintrag konnte nicht geöffnet werden.
1202	Registry Eintrag konnte nicht gelesen werden.
1203	Registry Eintrag konnte nicht geschrieben werden.
1204	Registry Eintrag konnte nicht entfernt werden.
1205	Registry Eintrag konnte nicht erzeugt werden.

Fehler-ID	Anzeige
1206	Kein Zugriff auf einen Systemdienst oder Treiber möglich.
1207	Ein Systemdienst oder Treiber konnte nicht in der Registry eingetragen werden.
1208	Ein Systemdienst oder Treiber konnte nicht aus der Registry entfernt werden.
1209	Ein Systemdienst oder Treiber ist bereits in der Registry eingetragen.
1210	Kein Zugriff auf den Service Control Manager möglich.
1211	Ein Eintrag für eine Session konnte in der Registry nicht gefunden werden.
1212	Ein Registry Eintrag ist ungültig oder falsch.
1301	Der Zugriff auf ein Laufwerk ist fehlgeschlagen.
1302	Keine Informationen über ein Laufwerk vorhanden.
1303	Kein Zugriff auf ein Volume möglich.
1304	Ungültige Option definiert.
1305	Unzulässiges Dateisystem.
1306	Das existierende Dateisystem auf einem Volume und das definierte sind unterschiedlich.
1307	Die vorhandene Größe eines Dateisystem-Clusters und die definierte Größe sind unterschiedlich.
1308	Unzulässige Sektorgröße eines Dateisystems definiert.
1309	Unzulässiger Startsektor definiert.
1310	Unzulässiger Partitionstyp definiert.
1311	Es konnte kein unfragmentierter, unbenutzter Bereich der erforderlichen Größe auf einem Volume gefunden werden.
1312	Dateisystem Cluster konnten nicht als benutzt markiert werden.
1313	Dateisystem Cluster konnten nicht als benutzt markiert werden.
1314	Dateisystem Cluster konnten nicht als unbenutzt markiert werden.
1315	Dateisystem Cluster konnten nicht als BAD markiert werden.
1316	Es existieren keine Informationen über die Cluster eines Dateisystems.

Fehler-ID	Anzeige
1317	Der als BAD markierte Bereich auf einem Volume konnte nicht gefunden werden.
1318	Unzulässige Größe eines Bereichs auf einem Volume definiert.
1319	Der MBR Sektor einer Festplatte konnte nicht ersetzt werden.
1330	Ein falsches Kommando für eine Allokierung oder Deallokierung definiert.
1351	Unzulässiger Algorithmus definiert.
1352	Der Zugriff auf den Systemkern ist fehlgeschlagen.
1353	Es ist kein Systemkern installiert.
1354	Beim Zugriff auf den Systemkern ist ein Fehler aufgetreten.
1355	Unzulässige Änderung der Systemeinstellungen.
1401	Auf ein Laufwerk konnten keine Daten geschrieben werden.
1402	Von einem Laufwerk konnten keine Daten gelesen werden.
1403	Der Zugriff auf ein Laufwerk ist fehlgeschlagen.
1404	Unzulässiges Laufwerk.
1405	Änderung der Zugriffsposition auf einem Laufwerk ist fehlgeschlagen.
1406	Laufwerk ist nicht bereit.
1407	Unmount eines Laufwerks ist fehlgeschlagen.
1451	Datei konnte nicht geöffnet werden.
1452	Datei konnte nicht gefunden werden.
1453	Unzulässiger Dateipfad definiert.
1454	Datei konnte nicht erzeugt werden.
1455	Datei konnte nicht kopiert werden.
1456	Keine Informationen über ein Laufwerk vorhanden.
1457	Die Position in einer Datei konnte nicht geändert werden.
1458	Das Lesen von einer Datei ist fehlgeschlagen.
1459	Es konnten keine Daten in eine Datei geschrieben werden.

Fehler-ID	Anzeige
1460	Eine Datei konnte nicht entfernt werden.
1461	Unzulässiges Dateisystem.
1462	Datei konnte nicht geschlossen werden.
1463	Kein Zugriff auf eine Datei möglich.
1501	Nicht genug Speicher vorhanden.
1502	Unzulässiger oder falscher Parameter definiert.
1503	Ein Puffer für Daten ist zu klein.
1504	Ein DLL-Modul konnte nicht geladen werden.
1505	Eine Funktion oder ein Prozess wurde abgebrochen.
1506	Kein Zugriff erlaubt.
1510	Es ist kein Systemkern installiert.
1511	Ein Programm konnte nicht gestartet werden.
1512	Eine Funktion, ein Objekt oder Daten sind nicht vorhanden.
1513	Unzulässiger Eintrag.
1514	Ein Objekt existiert bereits.
1515	Unzulässiger Funktionsaufruf.
1516	Es ist ein interner Fehler aufgetreten.
1517	Es ist eine Zugriffsverletzung aufgetreten.
1518	Funktion oder Modus wird nicht unterstützt.
1519	Deinstallation ist fehlgeschlagen.
1520	Es ist ein Ausnahmefehler aufgetreten.
1550	Der MBR Sektor der Festplatte konnte nicht ersetzt werden.
2850	Taskplaner-Dienst wurde wegen eines Ausnahmefehlers angehalten.
2851	Task-Planer Task erfolgreich ausgeführt
2852	Task-Planer Task fehlgeschlagen

Fehler-ID	Anzeige
2853	Task-Planer Task erzeugt oder geändert
2854	Task-Planer Task gelöscht
20001	Unbekannt
20002	Prozess beendet
20003	Datei nicht verifiziert
20004	Ungültige Richtlinie
30050	Die Anweisung Öffnen war nicht erfolgreich
30051	Nicht genug Speicherplatz
30052	Allgemeiner Fehler in der Prozess-Kommunikation
30053	Auf eine Ressource kann nicht zugegriffen werden. Das ist ein temporärer Zustand und ein späterer Versuch könnte erfolgreich beendet werden.
30054	Allgemeiner Kommunikationsfehler
30055	Unerwarteter Rückgabewert
30056	Kein Kartenlesegerät angeschlossen
30057	Zwischenspeicher überfüllt
30058	Karte ist nicht in Betrieb
30059	Eine Zeitüberschreitung ist eingetreten
30060	Unerlaubter Kartentyp
30061	Die gewünschte Funktionsart wird nicht unterstützt /zu dieser Zeit / In dieser OS / in dieser Situation.
30062	Ungültiger Treiber
30063	Die Firmware der angeschlossenen Hardware ist von dieser Software nicht nutzbar
30064	Öffnen der Datei ist fehlgeschlagen
30065	Datei nicht gefunden
30066	Karte nicht eingeführt

Fehler-ID	Anzeige
30067	Unzulässiges Argument
30068	Die Semaphore wird derzeit verwendet.
30069	Die Semaphore ist momentan in Benutzung
30070	Allgemeiner Fehler.
30071	Sie haben momentan nicht die Rechte, die angefragte Aktion durchzuführen. Normalerweise ist es notwendig zuvor ein Kennwort einzugeben.
30072	Der Service ist momentan nicht verfügbar.
30073	Ein Element (z. B. ein Schlüssel mit einem bestimmten Namen) konnte nicht gefunden werden.
30074	Das angegebene Kennwort ist falsch.
30075	Das Kennwort wurde mehrere Male falsch eingegeben und ist daher geblockt. Benutzen Sie ein Verwaltungstool, um dieses zu entsperren.
30076	Die Identität stimmt nicht mit der definierten Identitäts-Gegenprobe überein.
30077	Mehrere Fehler sind aufgetreten. Benutzen Sie diesen Fehlercode, wenn dies die einzige Möglichkeit ist, einen Fehlercode zu erhalten, aber vorher verschiedene Fehler aufgetreten sind.
30078	Einige Elemente sind noch vorhanden, daher kann z. B. die Verzeichnisstruktur etc. nicht gelöscht werden.
30079	Fehler während des Konsistenztestes
30080	Die ID ist auf der Schwarzen Liste. Die angefragte Aktion ist daher nicht erlaubt.
30081	Ungültiges Handle
30082	Ungültige Konfigurationsdatei
30083	Abschnitt nicht gefunden.
30084	Eintrag nicht gefunden.
30085	Keine weiteren Abschnitte vorhanden.
30086	Ende der Datei erreicht.
30087	Der angegebene Element existiert bereits.
30088	Das Kennwort ist zu kurz.

Fehler-ID	Anzeige
30089	Das Kennwort ist zu lang.
30090	Ein Element (z. B. ein Zertifikat) ist abgelaufen.
30091	Das Kennwort ist nicht gesperrt.
30092	Der Pfad konnte nicht gefunden werden.
30093	Das Datenverzeichnis ist nicht leer.
30094	Keine weiteren Daten verfügbar
30095	Auf dem Medium ist kein Speicherplatz mehr verfügbar.
30096	Eine Operation wurde abgebrochen.
30097	Read Only Daten; eine Schreiboperation ist fehlgeschlagen.
12451840	Der Schlüssel ist nicht verfügbar.
12451842	Der Schlüssel ist nicht definiert.
12451842	Zugriff auf unverschlüsseltes Medium verweigert.
12451843	Zugriff auf unverschlüsseltes Medium verweigert, wenn nicht es nicht leer ist.
352321637	Die Datei ist nicht verschlüsselt.
352321638	Der Schlüssel ist nicht verfügbar.
352321639	Der richtige Schlüssel ist nicht verfügbar.
352321640	Checksummenfehler im Datei-Header.
352321641	Fehler in CBI-Funktion.
352321642	Ungültiger Dateiname.
352321643	Fehler beim Lesen/Schreiben der temporären Datei.
352321644	Zugriff auf unverschlüsselte Dateien ist nicht erlaubt.
352321645	Key Storage Area (KSA) voll.
352321646	Die Datei ist bereits mit einem anderen Algorithmus verschlüsselt.
352321647	Datei ist mit NTFS komprimiert und kann daher nicht verschlüsselt werden!
352321648	Datei ist mit EFS verschlüsselt!

Fehler-ID	Anzeige
352321649	Ungültiger Datei-Besitzer!
352321650	Ungültiger Dateiverschlüsselungsmodus!
352321651	Fehler im CBC-Handling!
385875969	Integrität verletzt.
402653185	Das Token enthält keine Berechtigungen.
402653186	Berechtigungen können nicht auf das Token geschrieben werden.
402653187	TDF-Tag konnte nicht angelegt werden.
402653188	TDF-Tag enthält die angeforderten Daten nicht.
402653189	Das Objekt existiert bereits auf dem Token.
402653190	Kein gültiger Slot gefunden.
402653191	Seriennummer konnte nicht gelesen werden
402653192	Verschlüsselung des Tokens ist gescheitert.
402653193	Entschlüsselung des Tokens ist gescheitert.
536870913	Die Schlüsseldatei enthält eine ungültige Daten.
536870914	Teile des RSA-Schlüsselpaares sind ungültig.
536870915	Das Schlüsselpaar konnte nicht importiert werden.
536870916	Das Format der Schlüsseldatei ist ungültig.
536870917	Keine Daten verfügbar.
536870918	Der Import des Zertifikates ist fehlgeschlagen, da das Zertifikat bereits existiert.
536870919	Das Modul ist bereits initialisiert worden.
536870920	Das Modul ist nicht initialisiert worden.
536870921	Die ASN.1-Verschlüsselung ist fehlerhaft.
536870922	Fehlerhafte Datenlänge.
536870923	Fehlerhafte Signatur.
536870924	Fehlerhafter Verschlüsselungsmechanismus angewandt.

Fehler-ID	Anzeige
536870925	Diese Version wird nicht unterstützt.
536870926	Padding Fehler.
536870927	Ungültige Flags.
536870928	Das Zertifikat ist abgelaufen und nicht länger gültig.
536870929	Unkorrekte Zeitangabe. Zertifikat noch nicht gültig.
536870930	Das Zertifikat ist entzogen worden.
536870931	Die Zertifikats-Kette ist ungültig.
536870932	Die Zertifikats-Kette konnte nicht erstellt werden.
536870933	CDP konnte nicht kontaktiert werden.
536870934	Ein Zertifikat, welches nur als End-Dateneinheit genutzt werden kann, ist als CA oder umgekehrt genutzt worden.
536870935	Probleme mit der Gültigkeitslänge der Zertifikate in der Kette.
536870936	Fehler bei der Öffnung der Datei.
536870937	Fehler beim Lesen einer Datei.
536870938	Ein oder mehrere Parameter, die an die Funktion übergeben worden sind, sind nicht korrekt.
536870939	Die Ausgabe der Funktion passt nicht in den zur Verfügung gestellten Puffer.
536870940	Ein Problem mit dem Token und/oder Slot ist aufgetaucht.
536870941	Der Token hat nicht genug Speicherkapazität, um die gewünschte Funktion auszuführen.
536870942	Der Token ist aus dem Slot entfernt worden, während die Funktion ausgeführt wurde.
536870943	Die gewünschte Funktion konnte nicht ausgeführt werden, es liegen aber keine detaillierten Informationen über den Grund der Fehlermeldung vor.
536870945	Der Computer auf dem die CBI Sammlung läuft, besitzt ungenügenden Speicher, um die gewünschte Funktion auszuführen. Im schlechtesten Fall könnte es sein, dass die Funktion nur teilweise erfolgreich durchgeführt wird.
536870946	Eine gewünschte Funktion wird nicht vom CBI-Archiv unterstütz.

Fehler-ID	Anzeige
536870947	Es wurde versucht, einen Wert für ein Objekt einzustellen, welches nicht eingestellt oder abgeändert werden kann.
536870948	Ein ungültiger Wert wurde für ein Objekt angegeben.
536870949	Es wurde versucht, den Wert eines Objektes zu erlangen, was jedoch fehlschlug, da es sich um ein sensibles Objekt handelt bzw. es nicht extrahierbar ist.
536870950	Die angegebene OIN Lust abgelaufen. (Ob eine PIN eines normalen Benutzers auf einem ausgegebenen Token jemals abläuft, variiert von Token zu Token.)
536870951	Die angegebene PIN abgelaufen. Der Benutzer konnte nicht authentisiert werden.
536870952	Die angegebene PIN enthält ungültige Zeichen. Dieser Antwort-Code wird nur für Funktionen angewandt, die versuchen, eine PIN einzurichten.
536870953	Die angegebene PIN ist zu lang oder zu kurz. Dieser Antwort-Code wird nur für Funktionen angewandt, die versuchen, eine PIN einzurichten.
536870954	Die angegebene PIN ist geblockt und kann nicht genutzt werden. Dies tritt auf, weil eine gewisse Anzahl an fehlgeschlagenen Versuchen zur Authentisierung aufgetreten ist und der Token weitere Versuche zur Authentisierung ablehnt.
536870955	Die angegebene Slot ID ist ungültig.
536870956	Der Token war zu dem Zeitpunkt, als die Funktion angefragt wurde nicht in seinem Slot.
536870957	Das CBI Archiv und/oder der Slot konnte keinen Token im Slot erkennen.
536870958	Die angefragte Aktion kann nicht durchgeführt werden, da der Token schreibgeschützt ist.
536870959	Der angegebene Benutzer kann nicht angemeldet werden, da dieser Benutzername bereits zur Sitzung angemeldet ist.
536870960	Der angegebene Benutzer kann nicht angemeldet werden, da ein anderer Benutzer bereits zur Sitzung angemeldet ist.
536870961	Die gewünschte Aktion kann nicht ausgeführt werden, da der geeignete Benutzer (oder ein geeigneter Benutzer) nicht angemeldet ist. Zum Beispiel kann die Abmeldung von der Sitzung nicht vor der Anmeldung liegen.
536870962	Die normale Benutzer PIN ist nicht mit CBIInitPin initialisiert.
536870963	Es wurde versucht, gleichzeitig mehrere verschiedene Benutzer auf dem Token anzumelden, was der Token und/oder das Archiv zugelassen haben.
536870964	Ein ungültiger Wert wurde als CBIUser angegeben. Gültige Typen sind in ASCI11 User Types definiert.

Fehler-ID	Anzeige
536870965	Ein Objekt mit der angegebenen Kennzeichnung konnte auf dem Token nicht gefunden werden.
536870966	Eine Zeitüberschreitung ist aufgetreten.
536870967	Diese Version der IE ist nicht unterstützt.
536870968	Authentisierung fehlgeschlagen.
536870969	Das Root-Zertifikat ist gesichert.
536870970	Keine CRL gefunden.
536870971	Keine aktive Internetverbindung vorhanden.
536870972	Es befindet sich ein Fehler im Zeitwert eines Zertifikates.
536870973	Das Zertifikat konnte nicht verifiziert werden.
536870974	Der Aufhebungsstatus dieses Zertifikates ist unbekannt.
536870975	Das Modul wird beendet. Keine weiteren Anfragen gestattet.
536870976	Es ist ein Fehler während einer Netzwerkfunktion aufgetreten.
536870977	Ein ungültiger Aufruf einer Funktion ist empfangen worden.
536870978	Ein Objekt konnte nicht gefunden werden.
536870979	Eine Terminal Server Sitzung wurde unterbrochen.
536870980	Ungültige Handlung.
536870981	Das Objekt ist in Benutzung.
536870982	Der Zufallszahlengenerator wurde nicht initialisiert. (CBIRNDInit ( ) wurde nicht angefragt.)
536870983	Unbekannter Befehl (siehe CBIControl ( )).
536870984	UNICODE wird nicht unterstützt.
536870985	Der Zufallszahlengenerator benötigt einen größeren Startwert (seed).
536870986	Das Objekt existiert bereits.
536870987	Falsche Algorithmus Kombination. (Siehe CBIRecrypt ( )).
536870988	Das Cryptoki-Modul (PKCS#11) ist nicht initialisiert.

Fehler-ID	Anzeige
536870989	Das Cryptoki-Modul (PKCS#11) ist bereits initialisiert.
536870990	Das Cryptoki-Modul (PKCS#11) konnte nicht geladen werden.
536870991	Zertifikat nicht gefunden.
536870992	Nicht vertrauenswürdig.
536870993	Ungültiger Schlüssel.
536870994	Der Schlüssel ist nicht exportierbar.
536870995	Der angegebene Algorithmus wird momentan nicht unterstützt.
536870996	Der angegebene Entschlüsselungsmodus wird nicht unterstützt.
536870997	Ein Fehler in der GSENC Sammlung ist aufgetreten.
536870998	Format der Datenabfrage ist nicht bekannt.
536870999	Das Zertifikat hat keinen privaten Schlüssel.
536871000	Ungültige Konfiguration
536871001	Eine Operation ist aktiv.
536871002	Ein Zertifikat in der Kette ist zeitlich nicht verschachtelt.
536871003	Die CRL konnte nicht ersetzt werden.
536871004	Die BENUTZER-PIN wurde bereits initialisiert.
805306369	Sie haben keine ausreichenden Rechte, um diese Aktion auszuführen. Zugriff verweigert
805306370	Ungültige Handlung.
805306371	Ungültiger Parameter in Benutzung
805306372	Das Objekt existiert bereits.
805306373	Das Objekt konnte nicht gefunden werden.
805306374	Datenbank-Ausnahme aufgetreten.
805306375	Die Aktion wurde vom Benutzer abgebrochen.
805306376	Das Token ist keinem bestimmten Benutzer zugewiesen.

Fehler-ID	Anzeige
805306377	Das Token ist mehr als einem Benutzer zugewiesen.
805306378	Das Token konnte nicht in der Datenbank gefunden werden.
805306379	Das Token wurde erfolgreich gelöscht und aus der Datenbank entfernt.
805306380	Das Token konnte in der Datenbank nicht eindeutig identifiziert werden.
805306381	Die Richtlinie ist einer Richtlinien-Gruppe zugewiesen. Um die Richtlinie zu löschen, muss diese Zuweisung aufgehoben werden.
805306382	Die Richtlinie ist einer OU zugewiesen. Bitte entfernen Sie zuerst die Zuweisung.
805306383	Das Zertifikat dieses Beauftragten ist ungültig.
805306384	Das Zertifikat dieses Beauftragten ist abgelaufen.
805306385	Der Beauftragte konnte nicht in der Datenbank gefunden werden.
805306386	Der gewählte Beauftragte ist nicht eindeutig.
805306387	Der Beauftragte ist gesperrt und kann nicht authentisiert werden.
805306388	Der Beauftragte ist nicht mehr oder noch nicht gültig.
805306389	Der Beauftragte konnte nicht authentisiert werden - Anfrage außerhalb der gestatteten Arbeitszeiten.
805306390	Ein Beauftragter kann sich nicht selbst löschen.
805306391	Der Haupt-Sicherheitsbeauftragte kann nicht gelöscht werden, da ein zweiter Haupt-Sicherheitsbeauftragte zur zusätzlichen Authentisierung erforderlich ist.
805306392	Der Sicherheitsbeauftragte kann nicht gelöscht werden, da ein zweiter Sicherheitsbeauftragte zur zusätzlichen Authentisierung erforderlich ist.
805306393	Der Prüfungsbeauftragte kann nicht gelöscht werden, da ein weiterer Prüfungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306394	Der Recovery-Beauftragte kann nicht gelöscht werden, da ein Recovery-Beauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306395	Der Beratungsbeauftragte kann nicht gelöscht werden, da ein Beratungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306396	Die Funktion des Haupt- Sicherheitsbeauftragten kann nicht entfernt werden, da ein zweiter Haupt-Sicherheitsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.

Fehler-ID	Anzeige
805306397	Die Funktion des Sicherheitsbeauftragten kann nicht entfernt werden, da ein Sicherheitsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306398	Die Funktion des Prüfungsbeauftragten kann nicht entfernt werden, da ein Prüfungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306399	Die Funktion des Wiederherstellungsbeauftragten kann nicht entfernt werden, da ein Recovery-Beauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306400	Die Funktion des Beratungsbeauftragten kann nicht entfernt werden, da ein Beratungsbeauftragter zur zusätzlichen Authentisierung erforderlich ist.
805306401	Ein zusätzlicher Beauftragter mit der gewünschten Funktion ist zur zusätzlichen Authentisierung nicht verfügbar.
805306402	Ereignisanzeige
805306403	Integrität des zentralen Ereignisprotokolls erfolgreich verifiziert.
805306404	Integrität verletzt! Ein oder mehrere Ereignisse wurden vom Beginn der Kette entfernt.
805306405	Integrität verletzt! Ein oder mehrere Ereignisse sind in der Kette entfernt worden. Die Mitteilung bei der der Bruch der Kette entdeckt worden ist, ist hervorgehoben.
805306406	Integrität verletzt! Ein oder mehrere Ereignisse wurden vom Ende der Kette entfernt.
805306407	Exportieren der Ereignisse in Datei fehlgeschlagen. Grund:
805306408	Die momentane Ansicht enthält ungesicherte Daten. Möchten Sie die Änderungen speichern, bevor Sie die Ansicht verlassen?
805306409	Die Datei konnte nicht geladen werden, oder die Datei ist beschädigt. Grund:
805306410	Die Integrität des Protokolls ist verletzt worden! Ein oder mehrere Ereignisse sind entfernt worden.
805306411	Sollen die Ereignisse in einer Datei gesichert werden, bevor sie gelöscht werden?
805306412	Anzeige der Aufträge
805306413	CRL mehrfach in der Datenbank gefunden. CRL konnte nicht gelöscht werden.
805306414	CRL nicht in der Datenbank gefunden.
805306415	Der Benutzer, dem das Zertifikat zugewiesen werden sollte, konnte nicht in der Datenbank gefunden werden.
805306416	Ein P7 Blob ist für eine Zertifikats-Zuweisung zwingend erforderlich.

Fehler-ID	Anzeige
805306417	Der Benutzer, dem das Zertifikat zugewiesen werden sollte, ist nicht eindeutig benannt.
805306418	Die Zertifikats-Zuweisung kann nicht gefunden werden.
805306419	Die Zuweisung des Zertifikats ist nicht eindeutig. Es ist nicht klar, welche Zuweisung entfernt werden soll.
805306420	Der Benutzer für den das Zertifikat erstellt werden soll, konnte nicht in der Datenbank gefunden werden.
805306421	Der Benutzer für den das Zertifikat erstellt werden soll, kann nicht eindeutig benannt werden.
805306422	Das Zertifikat wurde bereits einem anderen Benutzer zugeordnet. Ein Zertifikat kann nur einem Benutzer zugeordnet werden.
805306423	Der Computer, dem das Zertifikat zugewiesen werden soll, konnte nicht in der Datenbank gefunden werden.
805306424	Der Computer, dem das Zertifikat zugewiesen werden soll, konnte nicht eindeutig identifiziert werden.
805306425	Importierte Zertifikate können nicht durch SGN erneuert werden.
805306426	Inkonsistente Zertifikatsdaten während der Erneuerung
805306427	Die Erneuerung des Zertifikats wurde nicht von einem Sicherheitsbeauftragten genehmigt.
805306428	Fehler beim Löschen des Token
805306429	Das Zertifikat kann nicht vom Token gelöscht werden, denn es wurde für die Authentisierung des aktuellen Benutzers verwendet.
805306430	Ein Systemzugang mit diesem Namen existiert bereits. Bitte wählen Sie einen anderen Namen.
805306431	Dem Sicherheitsbeauftragen sind keine Rollen zugewiesen. Anmeldung nicht möglich.
805306432	Die Lizenz wurde verletzt.
805306433	Es wurde keine Lizenz gefunden.
805306435	Fehlender oder ungültiger Protokolldateipfad
2415919104	Es wurde keine Richtlinie gefunden.
2415919105	Keine Konfigurationsdatei verfügbar!

Fehler-ID	Anzeige
2415919106	Keine Verbindung zum Server.
2415919107	Keine weiteren Datenpakete vorhanden.
2415919108	Ungültige Priorität beim Senden zum Server!
2415919109	Es stehen noch Daten zur Verarbeitung an.
2415919110	Die Autoregistrierung ist noch nicht beendet.
2415919111	Datenbank Anmeldung fehlgeschlagen.
2415919112	Falsche Session ID!
2415919113	Datenpaket ignoriert!
3674210305	Domäne nicht gefunden.
3674210306	Maschine nicht gefunden.
3674210307	Benutzer nicht gefunden.
3758096385	Das Kennwort enthält nicht genügend Buchstaben
3758096386	Das Kennwort enthält nicht genügend Zahlen
3758096387	Das Kennwort enthält nicht genügend Sonderzeichen
3758096388	Das Kennwort entspricht dem Benutzernamen
3758096389	Das Kennwort enthält aufeinanderfolgende Zeichen
3758096390	Das Kennwort ähnelt dem Benutzernamen zu stark
3758096391	Das Kennwort wurde in der Liste der verbotenen Kennwörter gefunden
3758096392	Das Kennwort ähnelt dem alten Kennwort zu stark
3758096393	Das Kennwort enthält eine Tastaturreihe mit mehr als zwei Zeichen
3758096394	Das Kennwort enthält eine Tastaturspalte mit mehr als zwei Zeichen
3758096395	Das Kennwort hat seinen Gültigkeitszeitraum noch nicht erreicht
3758096396	Das Kennwort hat seine Gültigkeitsdauer überschritten
3758096397	Das Kennwort hat seine minimale Gültigkeitsdauer noch nicht erreicht
3758096398	Das Kennwort hat die maximale Gültigkeitsdauer überschritten

Fehler-ID	Anzeige
3758096399	Information über einen bevorstehenden Wechsel des Kennwortes muß angezeigt werden
3758096400	Änderung bei Erstanmeldung erforderlich
3758096401	Das Kennwort wurde in der History gefunden
3758096402	Fehler beim Verifizieren gegen die spezifizierte Blacklist.
4026531840	Keine "platform" vorhanden.
4026531841	Kein Dokument.
4026531842	XML Parse Fehler.
4026531843	Fehler im Document Object Model (XML).
4026531844	Kein <DATAROOT>-Abschnitt gefunden (XML).
4026531845	XML-Tag nicht gefunden.
4026531846	"nostream" Fehler.
4026531847	"printtree" Fehler.

38.2 BitLocker Fehlercodes

BitLocker Fehler werden durch die folgenden SafeGuard Events gemeldet:

- 2072: Kernel-Initialisierung ist fehlgeschlagen. Interner Code: <Fehlercode>.
- 3506: Sektorbasierte Erst-Verschlüsselung des Laufwerks <*Laufwerksbuchstabe*> gescheitert und beendet. Grund: <*Fehlercode*>

Die folgende Tabelle enthält eine Liste von Fehlercodes für BitLocker:

Fehlercode (Hex)	**Fehlercode (Dec)**	**Beschreibung**
0x00000000 – 0x000032C8	0 – 15999	Siehe Microsoft Systemfehlercodes
0x00BEB001	12496897	Verschlüsselung ist aufgrund eines Fehlers während der Kernel-Initialisierung nicht möglich.
0x00BEB002	12496898	Der Boot Manager darf sich nicht auf dem zu verschlüsselnden Systemlaufwerk befinden.

0x00BEB003	12496899	Es wurde eine nicht unterstützte Windows Version gefunden. Minimum ist Windows Vista.
0x00BEB004	12496900	Die konfigurierte Authentisierungsmethode wird nicht unterstützt.
0x00BEB005	12496901	Der PIN Dialog wurde nicht erfolgreich abgeschlossen.
0x00BEB006	12496902	Der Pfad Dialog wurde nicht erfolgreich abgeschlossen.
0x00BEB007	12496903	Fehler in Kommunikation zwischen Prozessen des PIN oder Pfad Dialogs.
0x00BEB008	12496904	Unbehandelte Ausnahme im PIN oder Pfad Dialog. Der Dialog wurde angezeigt, aber der Benutzer meldete sich ab oder stoppte ihn im Task-Manager.
0x00BEB009	12496905	Der in der Richtlinie definierte Verschlüsselungsalgorithmus stimmt nicht mit dem des verschlüsselten Laufwerks überein. Standardmäßig (falls nicht geändert) verwendet die systemeigene BitLocker-Verschlüsselung AES-128, während die SGN Richtlinien AES-256 definieren.
0x00BEB00A	12496906	Das Volume ist ein schreibgeschütztes Volume. Dynamische Volumes werden nicht unterstützt.
0x00BEB00B	12496907	Der Hardware-Test ist aufgrund eines Hardwareproblems fehlgeschlagen.
0x00BEB00C	12496908	Bei der TPM-Initialisierung und -Aktivierung ist ein Fehler aufgetreten.
0x00BEB00D	12496909	Der Verschlüsselungsalgorithmus in der SGN-Richtlinie steht zu den Verschlüsselungsalgorithmus-Einstellungen im GPO in Konflikt.
0x00BEB102	12497154	Die UEFI Version konnte nicht überprüft werden, deshalb wird BitLocker im Legacy-Modus ausgeführt.
0x00BEB202	12497410	Das Client-Konfigurationspaket wurde noch nicht installiert.
0x00BEB203	12497411	Die UEFI Version wird nicht unterstützt und deshalb wird BitLocker im Legacy-Modus ausgeführt. Die Minimalanforderung ist 2.3.1.
0x80280006	-2144862202	Das TPM ist inaktiv.
0x80280007	-2144862201	Das TPM ist deaktiviert.
0x80280014	-2144862188	Das TPM hat bereits einen Besitzer.
0x80310037	-2144272329	Die Gruppenrichtlinieneinstellung, die FIPS-Konformität erfordert, verhindert, dass ein lokales Recovery-Kennwort erzeugt und in die Schlüssel-Backup-Datei geschrieben wird. Die Verschlüsselung wird dennoch fortgesetzt.

0x8031005B	-2144272293	Die Gruppenrichtlinie für die angegebene Authentisierungsmethode ist nicht gesetzt. Bitte aktivieren Sie die Gruppenrichtlinie "Zusätzliche Authentifizierung beim Start anfordern".
0x8031005E	-2144272290	Die Gruppenrichtlinie für Verschlüsselung ohne TPM ist nicht gesetzt. Bitte aktivieren Sie die Gruppenrichtlinie "Zusätzliche Authentifizierung beim Start anfordern" und aktivieren Sie darin das Kontrollkästchen "BitLocker ohne kompatibles TPM zulassen".
0x80280000 – 0x803100CF	-2144862208 – -2144272177	Siehe Microsoft COM Error Codes (TPM, PLA, FVE).

39 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie die SophosTalk-Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation/ herunter.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

40 Rechtliche Hinweise